ESCUELA SUPERIOR DE INGENIERÍA

INGENIERO TÉCNICO EN INFORMÁTICA

DE GESTIÓN

TRANSICIÓN DE UNA RED NO GESTIONADA A UNA RED SEGURA BASADA EN DISPOSITIVOS GESTIONABLES

Emilio J. Romero Díaz

Cádiz, Julio 2010

ESCUELA SUPERIOR DE INGENIERÍA

INGENIERO TÉCNICO EN INFORMÁTICA

DE GESTIÓN

TRANSICIÓN DE UNA RED NO GESTIONADA A UNA RED SEGURA BASADA EN DISPOSITIVOS GESTIONABLES

DEPARTAMENTO:	Ingeniería de Sistemas y Automática, Tecnología Electrónica y Electrónica
DIRECTOR DEL PROYECTO:	Carlos Rodríguez Cordón
AUTOR DEL PROYECTO:	Emilio J. Romero Díaz

Cádiz, Julio 2010

Fdo: Emilio J. Romero Díaz

Índice General

Capítulo 1. Introducción

Capítulo 2. Estudios Previos

Capítulo 3. Diseño de la LAN

Capítulo 4. Seguridad

Capítulo 5. Diseño de la WLAN

Capítulo 6. Configuración

Capitulo 7. Gestión de la red

Capítulo 8. Plan de pruebas

Capítulo 9. Conclusiones

Anexos

Bibliografía y referencias

Índice de figuras

Índice de tablas

Capítulo 1.
Introducción

1.1 Antecedentes

A medida que el flujo de información crece y los canales de comunicación aumentan su velocidad, las empresas se ven en la necesidad de mejorar su infraestructura de redes para su propio beneficio y el de sus clientes.

Las empresas son conscientes de la necesidad imperiosa de mejorar la infraestructura de sus comunicaciones, adaptándose a las nuevas tendencias del mercado, con objeto de aumentar considerablemente la eficiencia y el rendimiento de su red.

Una red debe ser rápida, estable, funcional, escalable, adaptable, flexible y de fácil administración. Uno de los factores más importantes para garantizar la velocidad y la confiabilidad de la red es, por tanto, el Diseño de la Red.

La elección de los equipos requiere un trabajo de ingeniería previo, puesto que en el mercado existen varias marcas competentes, como pueden ser Cisco, Juniper, Nortel, HP, 3COM, D-LINK. A la hora de realizar la inversión es importante tener en cuenta el Coste Total de la Propiedad (Total Cost of Ownership o TCO), ya que muchas veces la configuración y mantenimiento de los equipos conllevan costes muy superiores al de la adquisición inicial en sí.

El TCO, es un método de cálculo que permite determinar los costes directos e indirectos, así como los beneficios, relacionados con la compra de equipos o programas informáticos. Ofrece un resumen final que refleja no sólo el coste de la compra sino aspectos del uso y mantenimiento. Esto incluye formación para el personal de soporte y para usuarios, el coste de operación, y de los equipos o trabajos de consultoría necesarios, etc. Los estudios de TCO entre varios modelos ayudan a decidir qué equipo adquirir.

En este sentido, los estudios demuestran que Cisco es líder de mercado, incluso pese a que la empresa ha venido imponiendo su sistema operativo (Internetwork Operating System o IOS), en contrapunto con la tendencia del mercado de seguridad y networking basado en software libre.

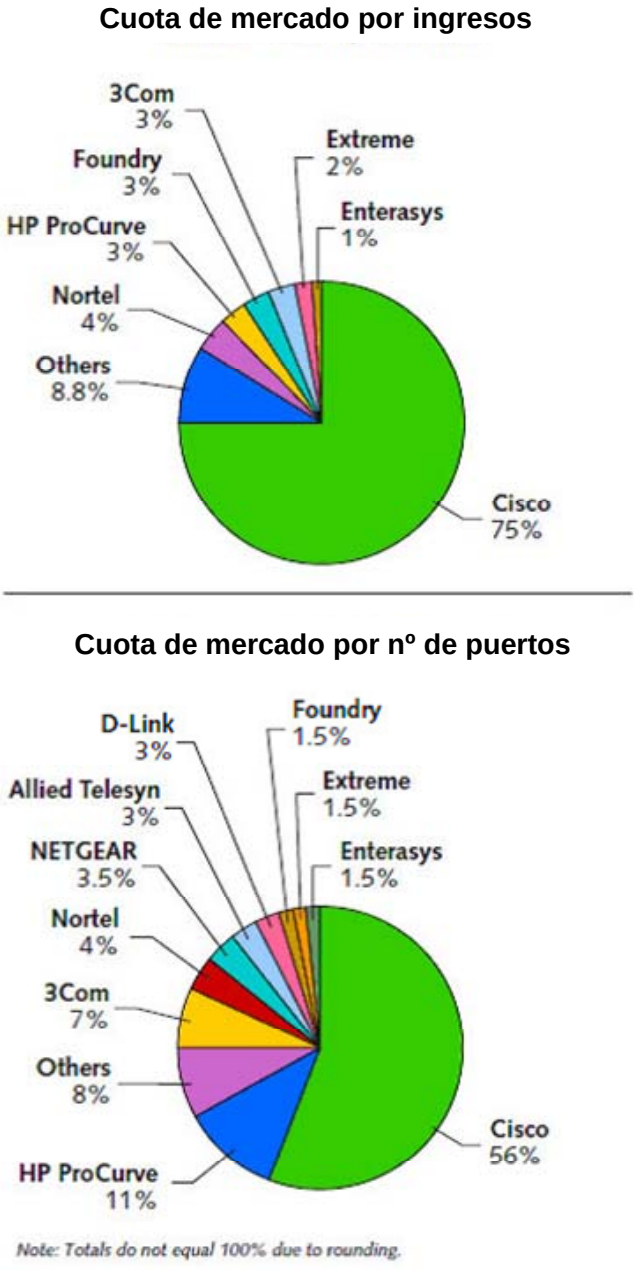


Figura 1- 1 CISCO líder en el mercado de la electrónica de red

La Figura 1-1 muestra que Cisco es propietaria del 56% de la cuota de mercado, atendiendo al número de puertos de la electrónica de red, con una friolera del 75% de los ingresos globales. La mayoría de los clientes se decantan por esta tecnología pues entienden que aunque el precio del equipamiento Cisco es mayor, su valor va más allá del precio de adquisición inicial.

HP ProCurve ocupa la segunda posición del mercado con un 11%, pero solo con un 3% del ingreso global. En este caso, un coste menor es el factor principal a la hora de comprar equipos de este fabricante.

En cuanto al mercado laboral, por el momento Cisco es la tecnología predominante, y para la que, a diferencia con otras marcas, resulta más sencillo encontrar técnicos cualificados, puesto que Cisco dispone de un gran número de academias regionales y locales distribuidas por todo el mundo, que facilitan la preparación del examen de certificación.

Este factor influye de manera significativa en el coste total de propiedad (TCO), reduciéndolo, ya que el número de profesionales formados en equipamiento Cisco excede claramente al de especialistas en cualquier otro fabricante, por lo que los técnicos de red "no-Cisco", debido a su escasez, pueden conseguir salarios entre un 10 y un 15% más altos.

Otra de las ventajas de Cisco frente a sus competidores es la existencia del centro de asistencia técnica (Cisco Technical Assistance Center o TAC), que proporciona apoyo técnico a sus productos, descarga de software, así como instalación, actualización, configuración, diseño, y resolución de problemas. Los estudios revelan que entre los criterios de selección tenidos en cuenta por los clientes, a la hora de elegir el fabricante de la electrónica de red, la disponibilidad de un buen centro de soporte es un factor decisivo.

Como muestra la siguiente figura, cuando se evalúa la tecnología para la electrónica de red, se debe realizar una previsión de las necesidades futuras de la empresa en un plazo mínimo de 5 años. Dado que por ejemplo, un producto con un coste total de propiedad (TCO) menor a principios del ciclo de vida, debido a que las empresas suelen necesitar nuevos servicios y realizar actualizaciones incrementales, puede conducir rápidamente a un incremento del TCO bastante elevado, mientras que otro equipo con un coste inicial mayor, sin embargo, puede mantener el crecimiento del TCO entre unos márgenes razonables.

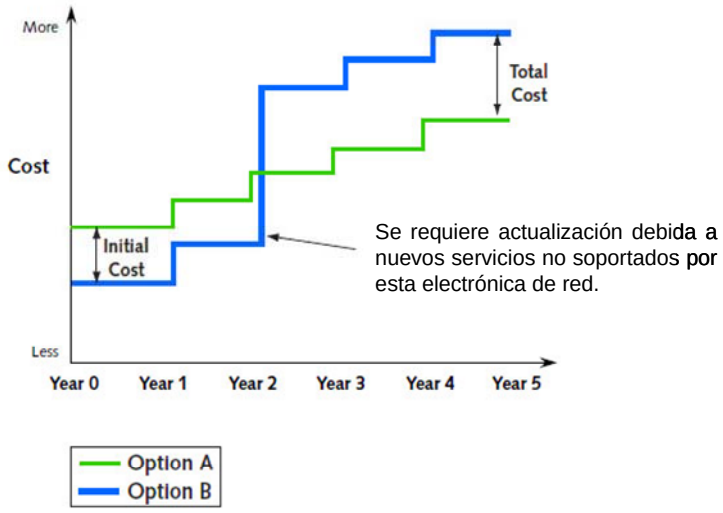


Figura 1- 2 Ejemplo de la evolución del TCO en 5 años

Las empresas que eligen Cisco saben que la inversión inicial de costes puede parecer engañosa. Es fácil de olvidar que el coste de la compra inicial de su red asciende típicamente al 20% de los costes totales de propiedad. A menudo, el 80% restante procede de los gastos de costes operacionales, mantenimiento y soporte. Sin embargo, con Cisco el coste total de propiedad (TCO) desciende, debido a la reducción de costes operacionales durante la vida del producto.

Tras el estudio anterior se llega a la conclusión de que integrar y expandir los servicios de seguridad de los routers y switches Cisco permite reducir el coste total de propiedad de la red (TCO) y obtener así un mayor retorno de la inversión.

Los switches, routers y el software de Cisco en conjunto crean una red integrada e inteligente que puede adaptarse a las necesidades actuales y futuras de cualquier empresa, ya que:

- Proporciona conectividad segura, pero sin obstáculos, entre los empleados, los clientes y la información.
- Proporciona aplicaciones de calidad y en tiempo real, como voz y vídeo en una plataforma de red convergente.
- Garantiza el acceso a la información y los recursos desde cualquier lugar.
- Automatiza una red gestionable y de autodefensa.
- Reduce los gastos operativos.
- Habilita prácticas ecológicas de negocios, Tecnología de la Información y redes.

Teniendo en cuenta todos estos aspectos, la evolución progresiva de este sector y con la intención de realizar un estudio que pueda ser perfectamente extrapolable al mercado actual, parece adecuado desarrollar un proyecto fin de carrera que presente previamente el análisis de una red basada en una electrónica de red no gestionable y desarrolle como solución a los problemas detectados, el diseño y la configuración de sus comunicaciones mediante dispositivos Cisco.

Aunque la aplicación de este estudio al mundo real es bastante amplia, se ha llevado a cabo tomando como referencia al Instituto Andaluz para la Tercera Edad (IATE)

El Instituto Andaluz para la Tercera Edad (IATE), es un Organismo Autónomo adscrito a la Consejería para la Igualdad y Bienestar Social de la Junta de Andalucía, de carácter administrativo y personalidad jurídica, autonomía administrativa y financiera. El IATE tiene encomendadas las siguientes funciones:

- La planificación, programación, organización, seguimiento y evaluación de las actuaciones dirigidas a la tercera edad, impulsadas por la Administración de la Junta de Andalucía, así como la colaboración con otras Administraciones Públicas y Entidades en el ámbito territorial de la Comunidad Autónoma de Andalucía.

- El fomento de la participación, promoción, información y formación dirigida a las personas mayores.

- La implantación del Carnet para la Tercera Edad, a través del cual el propietario puede beneficiarse de multitud de bienes y servicios en España y en el extranjero a un precio preferente.

- El desarrollo y la promoción del ocio y el turismo destinado a personas mayores, mediante la implementación de la Red de Instalaciones de Andalucía para la Tercera Edad, a través de la Empresa Pública de Instalaciones y Turismo INTURIMSERSO S.A.

- El fomento de la solidaridad y el voluntariado en cooperación con organizaciones y entidades juveniles.

- El establecimiento y gestión de centros de atención especializada.

- La implantación del programa de teleasistencia domiciliaria, a través del cual se ofrece apoyo inmediato a través de la línea telefónica a demandas de diversas órdenes; movilización de recursos ante situaciones de emergencia sanitaria; seguimiento permanente desde el Centro de Atención mediante llamadas telefónicas periódicas; y servicios de agenda, para recordar al usuario datos importantes sobre toma de medicación, realización de gestiones, etc.

Para poder llevar a cabo todas estas tareas el Instituto Andaluz para la Tercera Edad (IATE) físicamente se encuentra en Sevilla. Sin embargo, debido a la aceptación que están teniendo los servicios que ofrece y a la creciente demanda originada en otras provincias Andaluzas, está previsto en un futuro próximo la creación progresiva de diferentes delegaciones provinciales (DD.PP.), cuyas sedes estarían distribuidas por el resto de Andalucía. De ahí que con vista al futuro crecimiento, la sede de Sevilla haya sido ya rebautizada como Servicios Centrales (SS.CC.)

Como se comenta en el párrafo anterior, los servicios ofrecidos por el IATE han aumentado en los últimos tiempos, así como el número de trabajadores en la sede de Sevilla. Estos factores convierten al Instituto Andaluz para la Tercera Edad en candidato para la modernización de su

infraestructura de red, como medida básica para la prestación de servicios de forma óptima, y como soporte para las futuras tareas que realizan los profesionales que trabajan actualmente en SS.CC. y aquellos que lo harán en un futuro en sus diferentes DD.PP.

Actualmente la red interna de SS.CC. está totalmente cableada, no utiliza ningún tipo de tecnología inalámbrica, y no cuenta con línea de respaldo ni gestión de la red.

1.2 Red gestionada vs. Red no gestionada

El coste que supone cambios relevantes sobre la infraestructura de red ha puesto de moda adquirir dispositivos que puedan ser gestionados según las necesidades de la propia empresa, facilitando de esta manera un diseño óptimo de la electrónica de red, que permita posibles expansiones de dicha empresa sin suponer un nuevo impacto sobre su infraestructura.

A favor de la red no gestionada destacar la facilidad de su puesta en marcha y la reducción de costes. Su uso es ideal en empresas con pocos usuarios, y donde se requiera una conectividad básica. Por el contrario, dificulta la localización de errores, mantenimiento, administración y monitorización, e incluso compromete la seguridad de la compañía. Problemas que se pueden mitigar con una electrónica de red gestionada.

La red gestionable requiere una inversión mayor y la contratación de técnicos especializados, pero a cambio facilita la administración, configuración, mantenimiento y resolución de problemas, permitiendo realizar estas actividades remotamente. Y lo que es más, convierte a la red en una red segura, ya que aporta seguridad tanto física, permitiendo especificar quien se puede conectar a cada puerto, y que tipo de dispositivo puede hacerlo; como lógica, gracias a la segmentación mediante redes de área local virtuales (VLANs) y la utilización del protocolo Spanning Tree (STP).

La aplicación del protocolo STP, contribuye a aumentar la disponibilidad del sistema, ya que se encarga de calcular una topología optima de la red, deshabilitando enlaces redundantes, que generan bucles, y levantándolos en caso necesario.

Otro aspecto importante que mejora considerablemente en una red basada en elementos gestionables, es la monitorización de los dispositivos, gracias al uso del Protocolo Simple de Administración de Red (Simple Network Management o SNMP), o el protocolo NetFlow, en el caso de Cisco. Éste último permite llevar a cabo una monitorización más profunda, ofreciendo datos más elaborados que facilitan un análisis posterior mucho más completo.

Un ultimo punto a tener en consideración es que los switches gestionables están diseñados para redes con sobrecarga de tráfico, por lo que incorporan soporte integrado para tecnologías como calidad de servicio (Quality of Service o QoS), garantizando la transmisión de cierta cantidad de datos en un tiempo dado mediante la priorización del tráfico.

Con la aportación de todas estas características es evidente que los switches gestionables ayudan a mantener el tráfico y el rendimiento de la red con eficiencia y sencillez.

1.3 Objeto del proyecto

Tras el estudio de la situación actual de la empresa, basada en una electrónica de red no gestionable, el objetivo será buscar posibles mejoras y la puesta en marcha de una gestión de las comunicaciones con una electrónica de red de altas prestaciones, Cisco, persiguiendo obtener el máximo partido, con objeto de aumentar el rendimiento y seguridad de la red.

Durante este estudio, en el marco de las comunicaciones se procederá a estudiar los siguientes puntos:

- Diseño de la red
- Electrónica de red
- Sistemas de enrutamiento y direccionamiento.
- Comunicación inalámbrica
- Gestión de la red
- Seguridad

En el presente documento se describen detalladamente todos los trabajos realizados en la planificación, diseño, configuración, instalación y puesta en marcha de la red gestionable de SS.CC., así como las pertinentes pruebas para la comprobación de su correcto funcionamiento.

Aunque este proyecto fin de carrera se centra en SS.CC., con sede en Sevilla, y actualmente no existen las delegaciones provinciales, un requisito a tener en cuenta será que un plazo de dos años está planificado el despliegue del IATE por toda Andalucía, y que por tanto, la modernización a la que ahora se someta la infraestructura de red de SS.CC., debe ser realizada con vista a que la sede de Sevilla esté preparada para dar soporte al resto de delegaciones cuando llegue ese momento.

1.4 Estructura de la documentación

Este documento recoge el estudio realizado con el fin de alcanzar los objetivos anteriormente citados, y el resto de su contenido se ha estructurado de la siguiente manera:

- El capítulo 2, "Estudios Previos", presenta un análisis de la situación actual de la empresa y plantea las posibles mejoras para mitigar los problemas detectados.

- El capítulo 3, "Diseño de la LAN", se centra en la tecnología empleada, en la topología tanto física como lógica de la LAN, y la electrónica de red necesaria para el IATE. También define el subneting y el enrutamiento, y finalmente incluye un estudio detallado de cómo conseguir alta disponibilidad en las capas 2 y 3 del modelo OSI.

- El capítulo 4, "Seguridad", describe los ataques más comunes en la LAN y resalta las características que ofrece la electrónica de red de Cisco para mitigar dichos ataques. También trata la seguridad perimetral, el firewall, y los diferentes tipos de listas de control de acceso (ACL) como medida de seguridad en la red. Finalmente presenta las herramientas NTop y ARPWatch.

- El capítulo 5, "Diseño de la WLAN", se centra en el proceso seguido para conectar mediante enlace inalámbrico los tres edificios que constituyen la red de SS.CC. del IATE, plantenado la topología tanto física como lógica de la WLAN externa.

- El capítulo 6, "Configuración", describe la metodología utilizada para el despliegue de la LAN, la configuración realizada a la electrónica de red y a los puentes inalámbricos.

- El capítulo 7, "Gestión de la red", presenta una serie de herramientas de software libre de uso habitual para la gestión de la red.

- El capítulo 8, "Plan de pruebas", redacta las pruebas realizadas para verificar el cumplimiento de las especificaciones, el correcto funcionamiento de la red y el resultado de las mismas.

- El capítulo 9, "Conclusiones", como su título indica, expone las conclusiones finales y hace un análisis de las posibles líneas futuras, entre ellas, la incorporación de las DD.PP. a la red del IATE.

- Por último, se adjuntan una serie de anexos que incluyen presupuesto económico, hardware empleado, documentación de la red, y direccionamiento de las futuras DD.PP.

Capítulo 2.
Estudios Previos

2.1 Introducción

Este capítulo se dedica a describir un conjunto de actuaciones realizadas previamente a la fase de diseño de la red, objetivo de este proyecto. Estas actuaciones consisten básicamente en una inspección del lugar, identificando posibles zonas conflictivas y detectando las carencias que son responsables de los problemas actuales.

Finalmente, para cerrar el capítulo se enumera una serie de mejoras a implementar en el sistema, que dan solución a los conflictos detectados. Los puntos listados en esta última sección justifican la solución adoptada y se tomarán de base para el desarrollo de capítulos posteriores, en los que se tratará ampliamente cada uno de ellos.

2.2 Localización

Los SS.CC. del IATE tienen su sede en Sevilla, distribuida en tres edificios, ubicados en las direcciones resaltadas en el mapa.

Figura 2-1 Localización de edificios en Sevilla (SS. CC.)

Los edificios que constituyen los SS.CC. reciben el nombre de la calle donde residen.

- Edificio Muñoz Olivé en la calle Muñoz Olivé
- Edificio O'Donnell en la calle O'Donnell.
- Edificio Bilbao en la calle Bilbao.

2.3 Descripción del emplazamiento

Como se ha descrito anteriormente, la delegación de Sevilla está compuesta por tres edificios. El principal se encuentra en Muñoz Olivé y cuenta con una sola planta. El edificio Bilbao es de nueva construcción, y tiene tres plantas. Por último, O'Donnell dispone de dos plantas y es un edificio relativamente nuevo.

2.4 Análisis de la situación inicial

Previamente a cualquier tipo de actuación se presenta un estudio de la situación actual de la empresa. En este análisis se tienen en cuenta los siguientes puntos:

- Numero de usuarios
- Contabilización de rosetas de red
- Disponibilidad de la electrónica de red
- Numero de servidores
- Estructura de red actual
- Estudio del direccionamiento IP
- Comunicación entre las tres sedes
- Estudio de la Wireless externa

IATE, cuenta con una red de área local cableada para todas sus comunicaciones de datos que está actualmente en funcionamiento. La salida del edificio Principal, Muñoz Olivé, hacia la red corporativa, se realiza a través de una Marcrolan de 20 Mbps.

2.4.1 Número de usuarios

El número de usuarios de interés para el presente estudio, viene referido por el número de PCs en la red de la empresa.

- En la sede de Muñoz Olivé existe un total de 58 máquinas repartidas como sigue:
  - ✓ Recepción y Consejera: 12 PCs
  - ✓ Primer módulo: 15 PCs
  - ✓ Segundo módulo: 19 PCs
  - ✓ Tercer módulo e Informática: 10 PCs
  - ✓ Módulos del pasillo: 2 PCs

- En el Edificio Bilbao se dispone de 54 PCs repartidos de la siguiente forma:
  - ✓ Planta baja: 13 PCs
  - ✓ Planta primera: 12 PCs
  - ✓ Planta segunda: 21 PCs
  - ✓ Planta tercera: 8 PCs

- En el Edificio O'Donnell existen 35 PCs distribuidos como se indica a continuación
  - ✓ Planta baja: 15 PCs
  - ✓ Planta segunda: 20 PCs

2.4.2 Contabilización de rosetas de red

Durante la inspección se verifica que los edificios cuentan con un cableado estructurado certificado que da cobertura a todos los usuarios. No obstante, el estudio del cableado estructurado no es objeto del presente proyecto.

2.4.3 Disponibilidad de la electrónica de red

La electrónica de red en explotación actualmente se encuentra dividida en 4 Racks, dos en Muñoz Olivé, uno en Bilbao y otro en O'Donnell.

En Muñoz Olivé los Racks están ubicados uno en el pasillo, al que conectan los usuarios y las impresoras, y otro en el Centro de Proceso de Datos (CPD), al que conectan los servidores y el personal de informática. Los Racks de los Edificios Bilbao y O'Donnell sólo conectan usuarios y servidores. El contenido de estos Racks actualmente es el siguiente:

- Rack Pasillo Muñoz Olivé (RACK1)
  - ✓ 1 Switch Intel 24 puntos.
  - ✓ 1 Switch SMC 24 puntos.
  - ✓ 1 Hub Intel 24 puntos.
  - ✓ 1 Hub Intel de 16 puntos.
  - ✓ 1 Switch D-Link 24 puntos.
- Rack CPD Muñoz Olivé (RACK2)
  - ✓ 2 Switches SMC 24 puntos.
  - ✓ 1 Router Cisco 2800
  - ✓ 1 Router Cisco 2800 del proveedor.
- Rack Bilbao (RACK3)
  - ✓ 1 Switch Intel 24 puntos.
  - ✓ 2 Hubs Intel 24 puntos.
  - ✓ 1 Router Cisco 2800
- Rack O'Donnell (RACK4)
  - ✓ 1 Switch Intel 24 puntos.
  - ✓ 1 Switch SMC 24 puntos
  - ✓ 1 Router Cisco 2800

A continuación se muestran fotos de algunos de los Racks aquí mencionados, y más abajo algunas fotos ampliadas de los diferentes tipos de switches incorporados a los diferentes Racks.

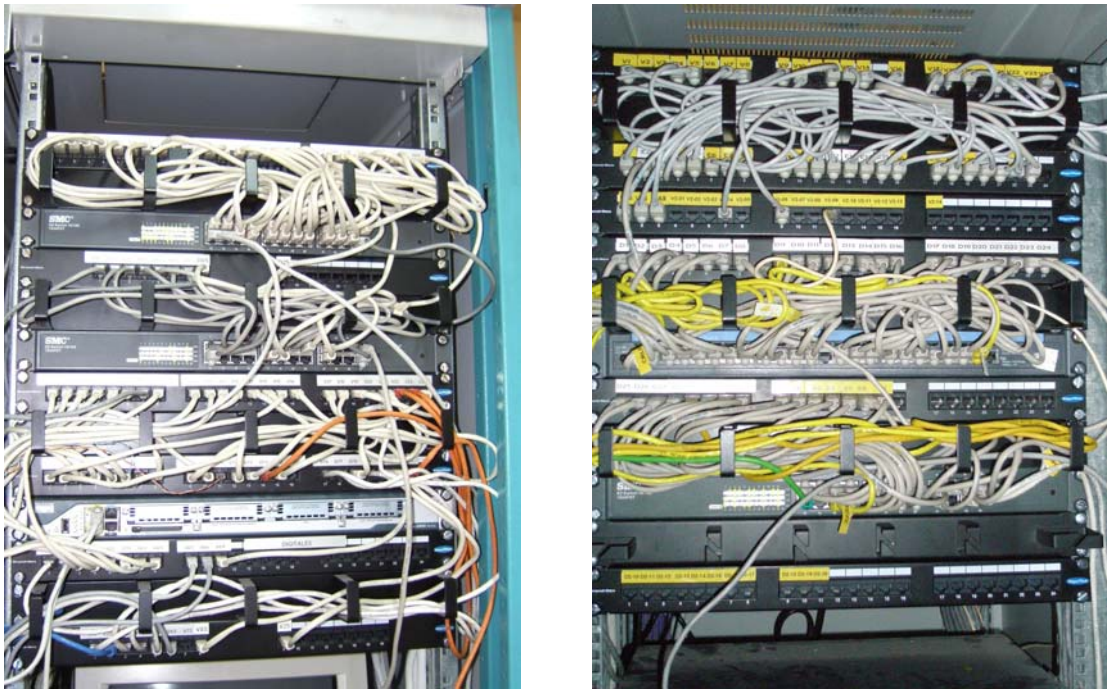


Figura 2-2 Rack 2-CPD Muñoz Olivé y Rack4-O'Donnell

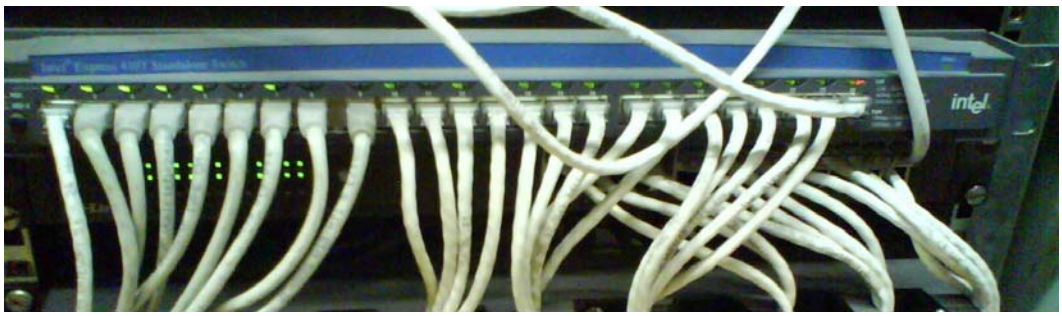


Figura 2-3 Switch Intel 24 puntos

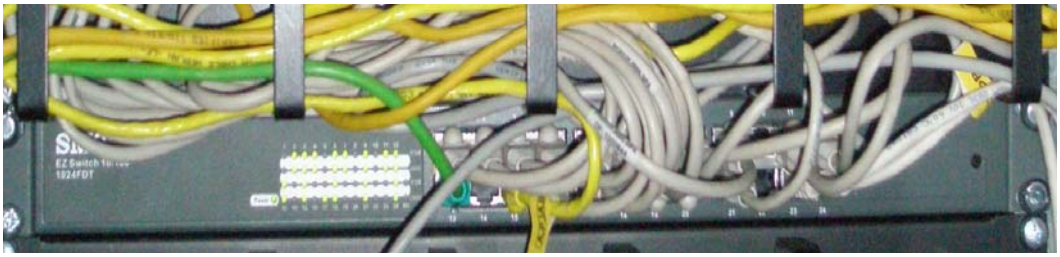


Figura 2-4 Switch SMC 24 puntos

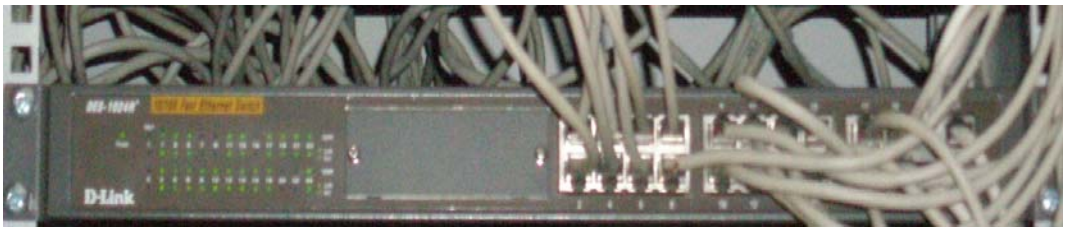


Figura 2-5 Switch D-Link 24 puntos

2.4.4 Numero de servidores

- En el sistema actual la distribución de los servidores en Muñoz Olivé es la siguiente:
  - ✓ Servidor dominio
  - ✓ Servidor impresión
  - ✓ Servidor base de datos
  - ✓ Servidor de ficheros
  - ✓ Servidor WEB
  - ✓ Servidor DNS
  - ✓ Servidor Proxy
  - ✓ Servidor de Backup
- En Bilbao y O'Donnell existe un controlador de dominio, impresión y backup

2.4.5 Estructura de red actual

Actualmente la estructura de red del IATE es no jerárquica, constituyendo la infraestructura más simple de red Ethernet. Este tipo de topología se conoce como red "plana", porque todo el tráfico que se transmite dentro de él es visto por todos los dispositivos interconectados, aunque no sean el destino de la transmisión.

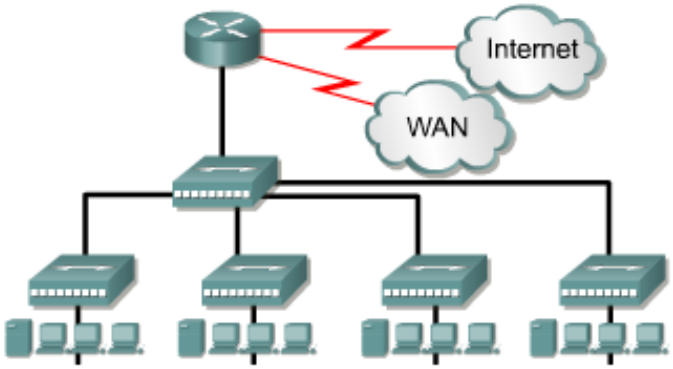


Figura 2-6 Estructura de red no jerárquica

A continuación se describen los dispositivos presentes en una red no jerárquica y sus funciones:

- Hub. Dispositivo de capa 1 usado para interconectar componentes de red como PC, impresoras, hubs y routers. Este dispositivo crea un único dominio de colisión y broadcast para todos los componentes de la red a la cual está conectado.

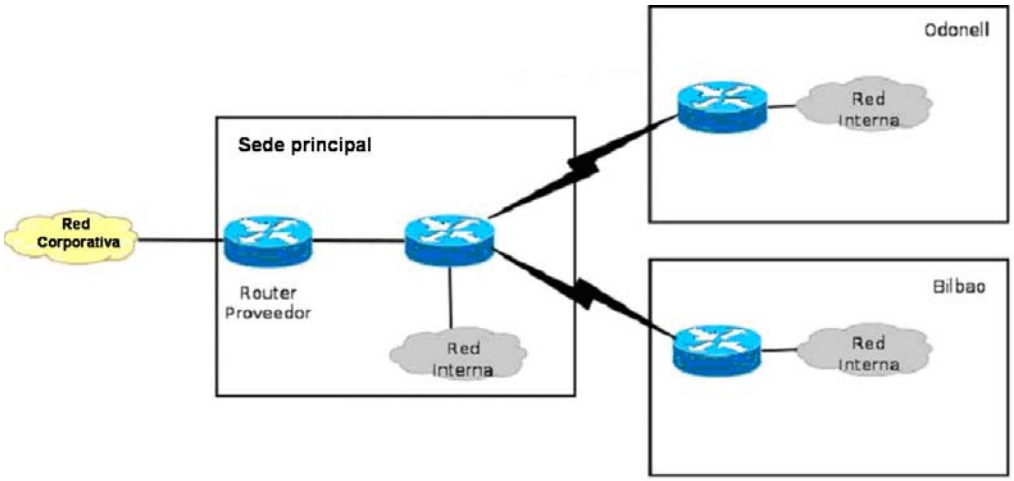
- Switch. Dispositivo de capa 2 usado para interconectar componentes como PC, impresoras, hubs y router. En su configuración por defecto, estos dispositivos crean un único dominio de broadcast para todo los dispositivos conectados a el. Cada puerto actúa como un dominio de colisión independiente.

- Router. Dispositivo de capa 3 usado para crear e interconectar segmentos de red o dominios de broadcast. Un router debe ser configurado antes que el tráfico pueda fluir a través de el. Cada interfaz crea un segmento de capa 3, por lo que establece el borde para los dominios de broadcast y de colisión para todos los dispositivos del segmento.

La infraestructura de red plana es muy sencilla de instalar y configurar, por lo que es una buena opción para redes domésticas y pequeñas oficinas. Sin embargo, en su contra, tiene como inconvenientes que compromete la seguridad de la compañía, no es escalable, mayor latencia de la red, y aumento del tráfico de difusión y del dominio de colisiones conforme se añaden nuevos dispositivos.

2.4.6 Estudio del direccionamiento IP

Antes de comenzar el desarrollo de este punto, se presenta el diseño lógico de la red de SS.CC.



LOCALIZACIÓN	TIPO	OBSERVACIÓN
Sevilla – Muñoz Olivé	Sede principal	Sede central, donde se encuentra los servidores principales
Sevilla - O'Donnell	Oficina	Se conecta a la sede Principal
Sevilla - Bilbao	Oficina	Se conecta a la sede Principal

Figura 2-7 Diseño Lógico de SS.CC

El direccionamiento IP privado otorgado al edificio principal y delegaciones en Sevilla es 10.239.64.0/18. Para la sede de Muñoz Olivé el direccionamiento es 10.239.64.0/24, mientras que para los Edificios Bilbao y O'Donnell el direccionamiento es 10.239.72.0/24 y 10.239.104.0/24, respectivamente. La conexión de cada edificio con la sede principal es punto a punto. La salida a Internet es proporcionada por la red corporativa.

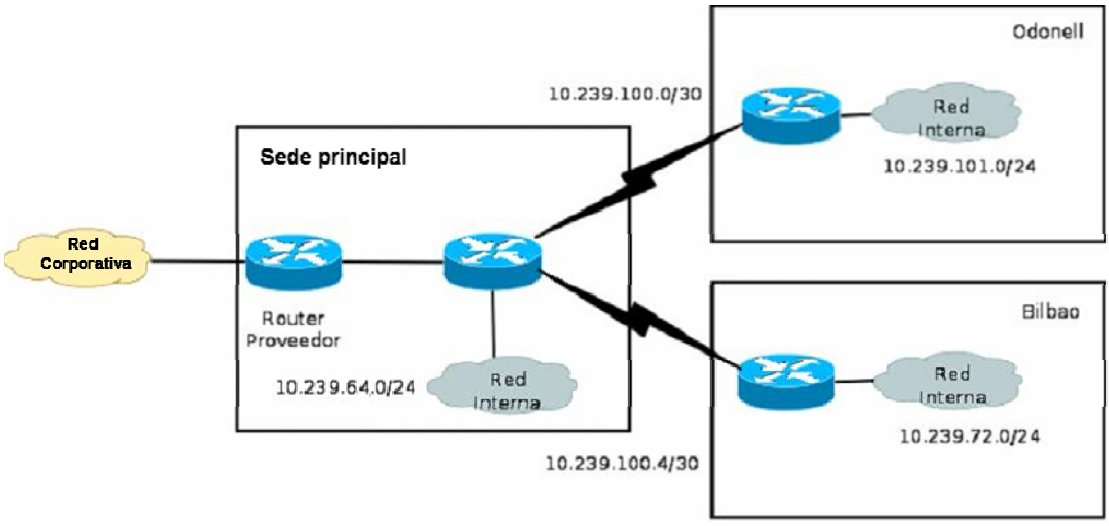


Figura 2-8 Direccionamiento IP de SS.CC.

2.4.7 Comunicación entre las tres sedes

Actualmente las sedes de Bilbao y O'Donnell, se conectan al edificio principal por líneas ADSL LAN to LAN de 10Mb. En cada sede se dispone de un servidor de archivo, y para proporcionar conectividad con las demás sedes, se utiliza un protocolo de enrutamiento dinámico, RIPv2.

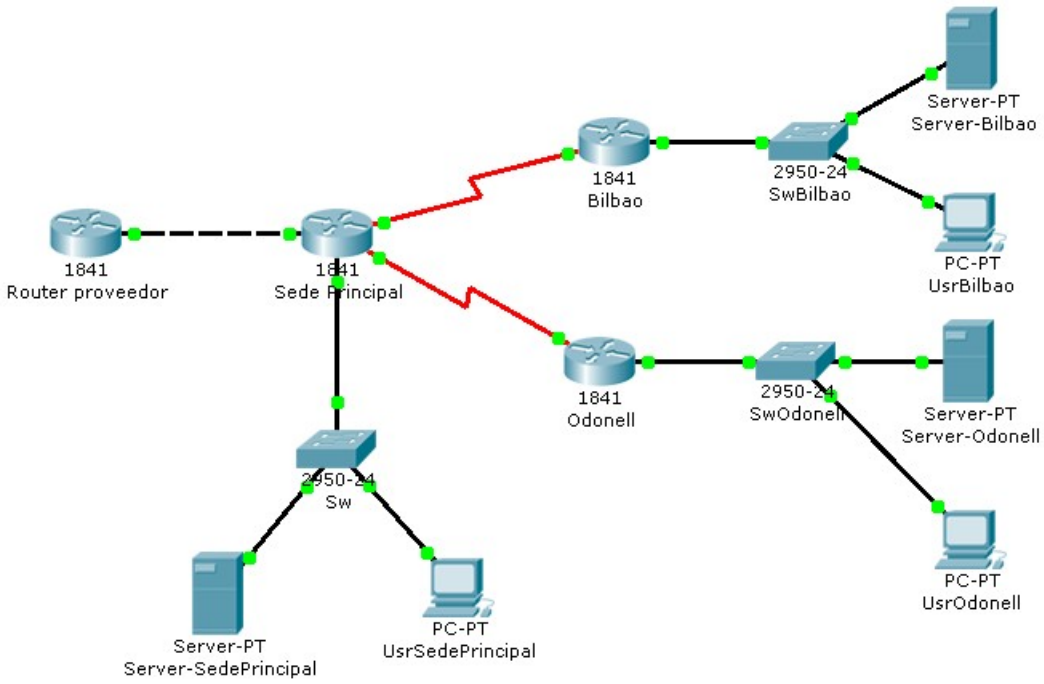


Figura 2-9 Diseño Físico de SS.CC.

2.4.8 Estudio de la Wireless externa

Actualmente la empresa no dispone de red inalámbrica.

2.5 Problemas detectados

Tras el estudio presentado en el apartado anterior, en este punto se listan las carencias encontradas.

1. En primer lugar, todos los inconvenientes derivados del uso de una topología de red no jerárquica, comentados en el punto 2.4.5: falta de mecanismos de seguridad, no escalabilidad, alta latencia, dificultad para encontrar errores, aumento del tráfico de difusión y del dominio de colisiones conforme se añaden nuevos dispositivos, causando como

consecuencia un exceso de utilización de los recursos de red y una reducción del rendimiento de la misma.

2. La electrónica de red dentro de los armarios se encuentra interconectada mediante latiguillos de cobre cruzados de 100Mbps, lo que supone un cuello de botella en la transmisión de datos entre los switches.

3. En Muñoz Olivé existe un Hub de 8 puntos, que da servicios a varias máquinas y conecta contra el rack del pasillo mediante un cable cruzado, detectándose pérdidas de conectividad debido a colisiones en Hub y provocando bloqueo de las máquinas conectadas al mismo.

4. En Bilbao también se detectan colisiones en los Hubs y bloqueo de los switches debido al calentamiento.

5. Actualmente no hay control sobre el ancho de banda usado por cada usuario, por lo que una única persona puede incluso saturar la red. En algunas ocasiones los usuarios realizan envíos de correos de gran tamaño provocando el bloqueo del cliente de correo, desencadenando la saturación de la red. Además no existe línea de backup contratada, con lo cual un fallo en la línea principal provoca la pérdida del servicio.

6. Se producen bucles en las sedes causado por un incorrecto parcheado. Esto es debido a que la electrónica de red no detecta los bucles, y como consecuencia provoca la pérdida de servicio en dichas sedes.

7. Como se pudo observar en la Figura 2-8, el direccionamiento actual no es el más óptimo, ya que el rango de red usado no es continuo, da un salto de la red 64 a la 72 y a la 104 del direccionamiento otorgado.

8. La comunicación entre las sedes se realiza usando líneas alquiladas, lo cual se traduce en un gasto económico considerable.

9. Debido a que la electrónica de red no es gestionable, no es posible deshabilitar las bocas en caso de que un equipo sea infectado por un virus, por lo que no hay forma de evitar la infección del resto de equipos.

10. No está implementado ningún mecanismo de seguridad, cualquier usuario puede pinchar su equipo en la red y obtener una dirección IP.

11. No existe ningún tipo de documentación sobre la red.

12. Finalmente, se anota también como una carencia importante, el hecho de que no exista ningún tipo de gestión de red, puesto que dificulta considerablemente los trabajos de control del estado de la red.

2.6 Mejoras a implantar en el sistema.

Para finalizar, este apartado presenta una visión general de las medidas que se llevarán a cabo con el fin de afrontar los problemas descritos anteriormente y mejorar el actual sistema, resumiendo al mismo tiempo los beneficios que se obtendrán con cada una de estas decisiones.

- **Implantación de una estructura de red jerárquica**. Gracias a esta acción se evolucionará hacia una red determinista con límites claramente definidos entre los módulos y con puntos de demarcación que permitirán al diseñador saber exactamente dónde se localiza el tráfico.

  La topología jerárquica proporciona escalabilidad, permitiendo a las empresas añadir módulos fácilmente, y facilita la tarea de diseño haciendo cada módulo independiente. Pero además, mientras crece la complejidad de la red, los diseñadores pueden añadir nuevos módulos funcionales. Por otro lado, ofrece mayor integridad en el diseño de la red, permitiendo añadir servicios y soluciones sin cambiar el diseño subyacente.

  Esta mejora es fundamental con vistas al futuro despliegue de las DD.PP. por Andalucía.

- **Modificaciones en el subneting de la red y creación de VLANs**. Mediante la implementación y el uso de VLANs se reducirá el impacto de los broadcast en la red y se conseguirá una independencia física siguiendo una organización lógica. Por otra parte, la segmentación facilitará la detección de errores y disminuirá la latencia de la red.

- **Creación de enlaces rápidos para servidores**. Con esta medida se evitarán cuellos de botella a la hora de acceder a los servidores.

- **Seguridad a nivel físico**. Saber quién está conectando y dónde, resulta fundamental para aumentar la seguridad interna de la compañía. La seguridad a nivel físico permitirá especificar quien y que tipo de dispositivo puede conectarse a cada puerto.

- **Seguridad en la LAN**. En la mayoría de las ocasiones gran parte de los ataques provienen del interior de la organización, la protección a nivel de capa 2 mitigará los ataques mas comunes a nivel de enlace, como pueden ser Address Resolution Protocol (ARP) Spoofing, Media Access Control (MAC) Flooding, Dynamic Host Configuration Protocol (DHCP) Snooping, VLAN Hooping, etc.

- **Seguridad Perimetral**. Establecimiento de recursos de seguridad en el perímero de la red a través de firewall.

- **Actualización/Adquisición de electrónica de red**. La adquisición de dispositivos gestionables facilitará la administración, configuración, mantenimiento y resolución de problemas, permitiendo realizar estas actividades remotamente.

- **Generar y mantener la documentación de la red.** Una buena documentación de la red permitirá obtener rápidamente información sobre un dispositivo determinado, además de servir como referencia para analizar, comparar y verificar el estado de la red.

- **Implantación de la gestión de la red.** La gestión de la red reducirá la indisponibilidad de la red y optimizará su rendimiento para poder aprovechar los recursos al máximo.

- **Uso de Wireless Externa.** El uso de enlaces inalámbricos para la unión entre dos edificios reducirá el gasto que suponen las líneas alquiladas.

- **Contratación de una línea de backup.** Permitirá mantener el servicio de manera ininterrumpida.

Con estas medidas se conseguirá un rendimiento óptimo de la red, así como agilizar la transferencia de datos. Cada uno de estos puntos se desarrollará detalladamente en capítulos posteriores del presente documento.

2.7 Plan de actuación

A continuación se detallan las acciones que se llevarán a cabo para proceder a mejorar la infraestructura de red del IATE, así como el tiempo estimado para realizar cada una ellas.

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**FASE DE ANALISIS Y ESTUDIOS PREVIOS**	**14 días**	**vie 19/02/10**	**mié 10/03/10**
2	Planteamiento del problema	0 días	vie 19/02/10	vie 19/02/10
3	Análisis de la situación inicial	7 días	lun 22/02/10	mar 02/03/10
4	Declarar problemas	2 días	mié 03/03/10	jue 04/03/10
5	Plantear mejoras	2 días	vie 05/03/10	lun 08/03/10
6	Elaboración Presupuesto	2 días	mar 09/03/10	mié 10/03/10
7	Aceptación del proyecto y presupuesto	0 días	mié 10/03/10	mié 10/03/10
8	**FASE DE DISEÑO**	**12 días**	**jue 11/03/10**	**vie 26/03/10**
9	Diseño de la LAN	6 días	jue 11/03/10	jue 18/03/10
10	Diseño de la WLAN	2 días	vie 19/03/10	lun 22/03/10
11	Plan de seguridad	4 días	mar 23/03/10	vie 26/03/10
12	Pedido del material	0 días	lun 22/03/10	lun 22/03/10
13	**FASE DE INSTALACION**	**27 días**	**mar 23/03/10**	**sáb 24/04/10**
14	Acopio de material	22 días	mar 23/03/10	lun 19/04/10
15	Instalación Antenas externas	1 día	mar 20/04/10	mar 20/04/10
16	Instalación de la electronica de red	1 día	sáb 24/04/10	sáb 24/04/10
17	Conexionado	1 día	sáb 24/04/10	sáb 24/04/10
18	Instalación de puentes inalámbricos	1 día	mar 20/04/10	mar 20/04/10
19	**FASE DE CONFIGURACION**	**11 días**	**mar 20/04/10**	**vie 30/04/10**
20	Configuración de la electronica de red	4 días	mar 20/04/10	vie 23/04/10
21	Configuración de puentes inalámbricos	1 día	vie 23/04/10	vie 23/04/10
22	Migración de servidores	1 día	dom 25/04/10	dom 25/04/10
23	Configuración de la gestión de red	5 días	lun 26/04/10	vie 30/04/10
24	**FASE DE PUESTA EN MARCHA Y CERTIFICACION**	**6 días**	**lun 26/04/10**	**lun 03/05/10**
25	Puesta en marcha	5 días	lun 26/04/10	vie 30/04/10
26	Pruebas de verificación	6 días	lun 26/04/10	lun 03/05/10

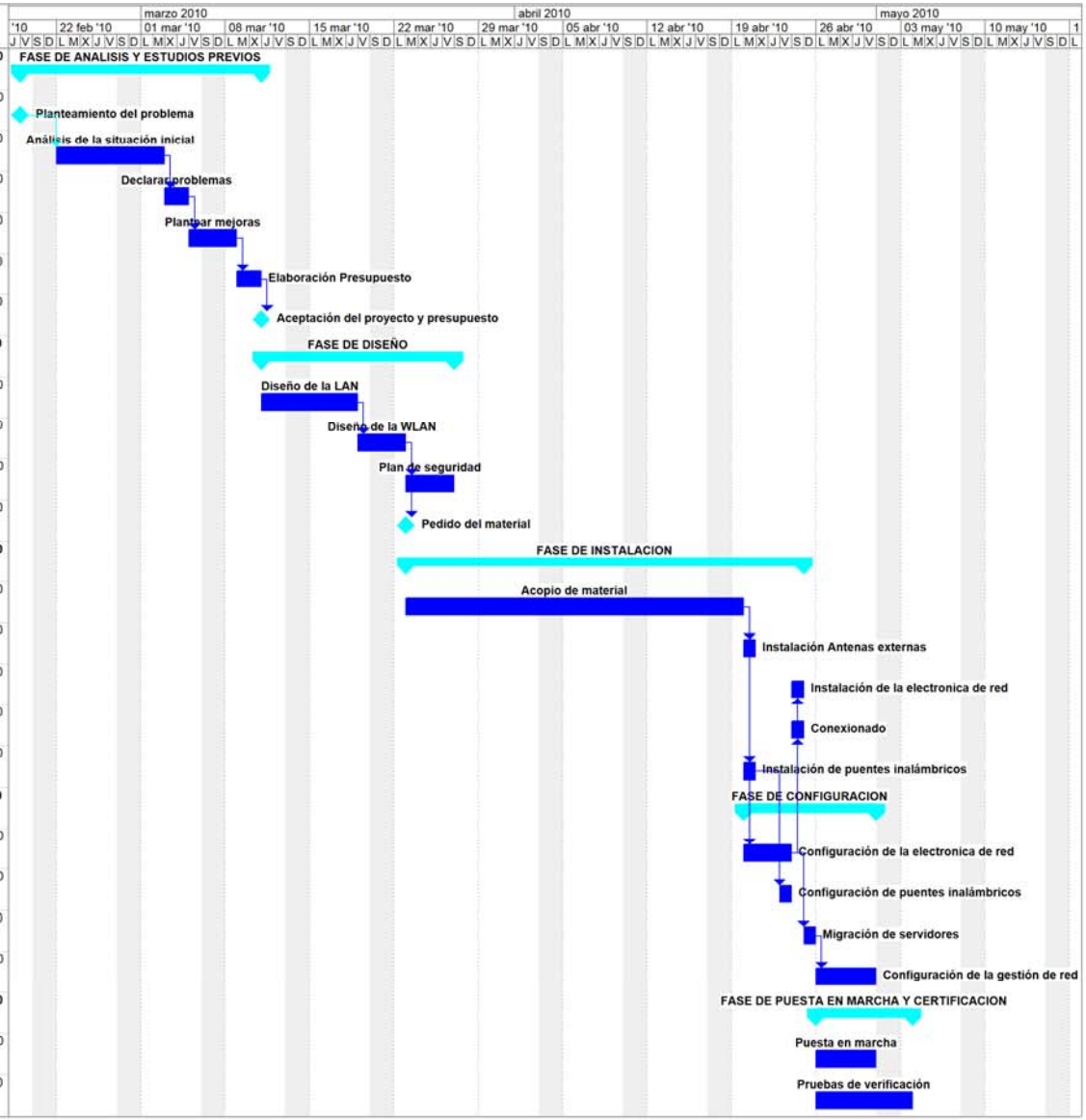


Figura 2-10 Plan de actuación

2.8 Conclusiones

A lo largo de este capítulo se han recopilado datos reales, resultados del estudio previo llevado a cabo en las instalaciones del IATE, en cuanto al número de usuarios, la disponibilidad de la electrónica de red, el direccionamiento IP, la estructura de red, y la comunicación entre las sedes.

El análisis de estos datos ha puesto en evidencia las deficiencias existentes en la red actual del IATE, tales como alta latencia, colisiones, pérdidas de conectividad, direccionamiento IP ineficiente, bajo rendimiento, falta de mecanismos de seguridad, ausencia de documentación de red, y dificultad para la monitorización de errores. Y lo que es aún peor, una estructura de red no jerárquica, que entre otras cosas, impide la escalabilidad de la empresa, uno de los principales motivos por los cuales el IATE se ve en la necesidad de adaptar su infraestructura de red.

Finalmente, una vez identificados los problemas, se han definido en líneas generales las medidas adoptadas con el fin de aumentar el rendimiento y la seguridad, todas ellas orientadas hacia el uso de una electrónica de red gestionable. Estas decisiones de diseño constituyen la base para el resto de capítulos del presente documento y se considerarán el punto de partida para iniciar un nuevo diseño de la LAN, basado en una topología de red jerárquica y en el uso de dispositivos gestionados.

Capítulo 3.
Diseño de la LAN

3.1 Introducción

Esta sección se dedica a detallar el proceso de diseño de la LAN del IATE y a describir las decisiones tomadas al respecto. Su principal objetivo consiste en determinar el diseño más adecuado para la organización.

El capitulo comienza presentando el modelo de referencia adoptado y la arquitectura de red propuesta, tanto lógica como física. Seguidamente se describe el equipamiento usado, así como su localización y conexionado, y se determina el direccionamiento más apropiado para la red. Finalmente se trata extensamente el tema de la redundancia en capa 2 y 3.

Sin embargo, el proceso de diseño de la LAN abarca también los dos próximos capítulos, Seguridad y Diseño de la WLAN (Wireless LAN). Una vez establecido el diseño a partir de los puntos cubiertos a lo largo de estos tres capítulos, se podrá pasar a la fase de implementación de la LAN.

3.2 Definición de los componentes de la red

Una red de datos ayuda a una organización a incrementar la productividad enlazando todas las computadoras y redes para que los usuarios tengan acceso a la información independientemente del momento del día, su localización o el tipo de equipamiento.

Las redes de datos han cambiado la forma de ver las empresas y los empleados. Actualmente las compañías organizan sus redes corporativas de modo que les permita optimizar sus recursos. La Figura 3-1 muestra la tendencia actual de las empresas en cuanto a estructura de red, basándose en una agrupación de usuarios del siguiente modo:

- La oficina central es el punto al que todos están conectados a una LAN y donde está localizada la mayor parte de la información corporativa. Puede tener cientos o miles de usuarios que dependen de la red para llevar a cabo su trabajo, y suele ser un edificio con

muchas LAN o un campus que agrupe varios edificios. Ya que todo el mundo necesita acceder a los recursos centralizados y a la información, suele disponer de un núcleo (backbone) LAN de alta velocidad, así como de un centro de datos centralizado con mainframes y servidores de aplicaciones.

- Las otras conexiones son una variedad de localizaciones de acceso remoto que conectan con los recursos de la oficina central y entre ellas.

  - Sucursales: Localizaciones externas en las que trabajan un pequeño grupo de personas, que se conectan entre sí a través de una LAN, mientras que para acceder a la oficina central usan servicios WAN. Aunque parte de la información puede encontrarse en la propia sucursal, la mayoría de los datos a los que acceden estos usuarios se encuentran en la oficina central.

  - Teletrabajadores. Empleados que trabajan desde sus propios domicilios y a la hora de acceder a los recursos de la red suelen conectarse bajo demanda a la oficina central y a las sucursales.

  - Usuarios móviles. Empleados que trabajan en distintas localizaciones y cuentan con distintos servicios para conectarse a la red. Cuando están en la oficina central o en una sucursal emplean la LAN corporativa, mientras que si se encuentran fuera de estas localizaciones emplean servicios de marcación o enlaces de acceso a Internet de alta velocidad para conectar con la red corporativa usando servicios VPN (Virtual Private Network o Red privada virtual).

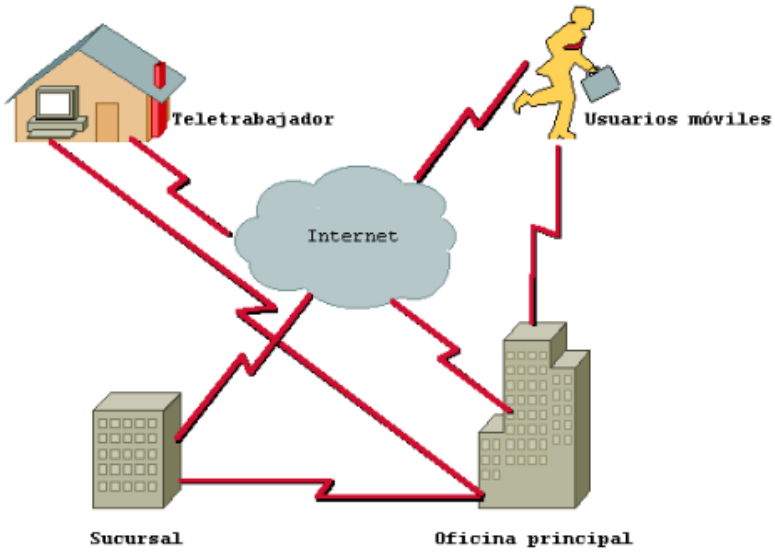


Figura 3-1 Estrategia de red corporativa

Para conocer el tipo de equipamiento y los servicios que se deben implementar en el IATE, es importante comprender las necesidades de la empresa y de los usuarios. Para ello, resulta útil subdividir la red en un modelo jerárquico que abarque desde la maquina del usuario final hasta el núcleo (backbone) de la red.

La jerarquía tiene muchos beneficios en el diseño de las redes y ayuda a hacerlas más predecibles. En si, define funciones dentro de cada capa, ya que las redes grandes pueden ser extremadamente complejas e incluir múltiples protocolos y tecnologías.

En el presente proyecto se utilizará el modelo jerárquico de tres capas de Cisco, descrito en los siguientes apartados, para dividir la red en componentes más pequeños. De este modo, se obtendrá un modelo de red fácilmente entendible que ayudará a decidir una manera apropiada de aplicar una configuración.

3.3 Modelo Jerárquico

Con el fin de simplificar el diseño, implementación y administración de las redes, Cisco utiliza un modelo jerárquico para describir la red. Aunque el modelo suele estar asociado concretamente con el proceso de diseño de la red, es importante comprenderlo desde las primeras fases del proyecto para poder determinar que equipo y que características son necesarias en la misma.

Las demandas de los usuarios y de las aplicaciones de red han obligado a los profesionales de la red a emplear patrones de tráfico como criterio para construir un internetworking. Las redes no pueden ser divididas en subredes basándose únicamente en el número de usuarios. La aparición de servidores capaces de ejecutar aplicaciones globales tiene también un impacto directo en la carga de la red. Un tráfico elevado supone tener que emplear técnicas de conmutación y enrutamiento más eficientes.

Hoy día los patrones de tráfico dictan el tipo de servicios que los usuarios finales precisan en la red. Para construir un internetworking que satisfaga las necesidades de estos usuarios, se emplea un modelo jerárquico de tres capas para organizar el flujo de tráfico.

Como representa la siguiente figura, el modelo está compuesto por tres capas, que son la de acceso, la de distribución y la capa núcleo. Cada una de ellas cumple una función en el suministro de servicios de red.

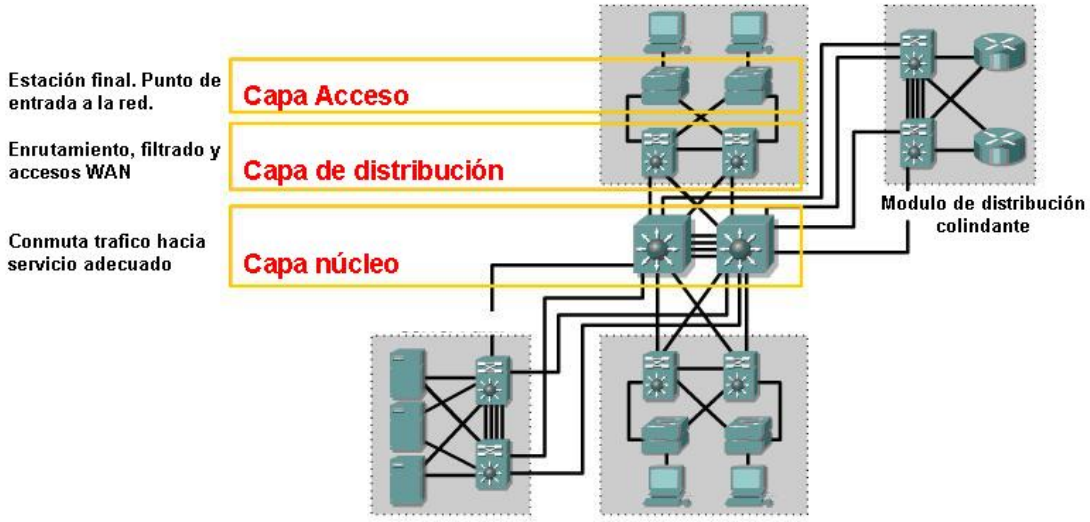


Figura 3-2 Modelo de red jerárquico de tres capas

3.3.1 Capa de acceso

La capa de acceso de la red es el punto en el que cada usuario se conecta a la red, razón por la cual recibe a veces el nombre de capa escritorio. Los usuarios, así como los recursos a los que estos necesitan acceder con más frecuencia, están disponibles a nivel local. El tráfico hacia y desde recursos locales está confinado entre los propios recursos, los switches y los usuarios finales. En la capa de acceso existen múltiples grupos de usuarios junto con sus recursos.

En muchas redes, no es posible ofrecer a los usuarios acceso local a todos los servicios, como bases de datos, almacenamiento centralizado o acceso a la Web. En estos casos, este tipo de trafico se redirige a la siguiente capa del modelo, la de distribución.

3.3.2 Capa de distribución

La capa de distribución marca la frontera entre la capa de acceso y los servicios básicos de la red. Su tarea principal es llevar a cabo las tareas de enrutamiento, filtrado y acceso a WAN. Entres sus funciones destacan las siguientes:

- Servir como punto de concentración para los dispositivos de la capa de acceso.
- Enrutar el tráfico para proporcionar acceso por departamentos o grupos de trabajo.
- Ofrecer servicios de seguridad y filtrado.

La capa de distribución puede resumirse como la capa que ofrece conectividad basada en políticas, ya que determina la forma en la que los paquetes pueden acceder a los servicios básicos de la red, y si realmente pueden acceder a ellos. También determina la vía más rápida para que una petición de usuario (como el acceso a un servidor de ficheros) sea reenviada al servidor. Una vez que esta capa escoge la ruta, reenvía esa petición a la capa núcleo, la cual entonces la trasportará rápidamente al servicio apropiado.

3.3.3 Capa núcleo

Como se ha dicho anteriormente, esta capa, también conocida como capa backbone, dirige el tráfico al servicio apropiado tan rápido como sea posible. Normalmente, dicho tráfico se dirige o proviene de servicios comunes a todos los usuarios y reciben el nombre de servicios globales o corporativos, como por ejemplo el correo electrónico o el acceso a Internet.

Cuando un usuario precisa acceder a un servicio corporativo, la petición se procesa a nivel de la capa de distribución. Esta reenvía a continuación dicha solicitud al backbone, el cual se limita a proporcionar un transporte rápido hasta el servicio solicitado. El dispositivo de la capa de distribución se encarga de suministrar acceso controlado al núcleo.

En redes más pequeñas, no es inusual que se implemente un modelo de núcleo colapsado, en el que se combinan la capa de distribución y la capa núcleo en una única capa.

3.3.4 Aplicación del modelo jerárquico al IATE

Como se dijo en el capítulo anterior, la oficina central se encuentra en la sede de Muñoz Olivé y a ella se conectan el resto de sedes para tener acceso a los recursos centralizados. Por tanto, en la sede principal, Muñoz Olivé, se encuentra el backbone de la red, la capa núcleo, donde se localizan los servicios principales a los que van a acceder los usuarios del resto de sedes. En realidad, se trata de un modelo de núcleo colapsado, en el que se combinan capa de distribución y capa núcleo en una misma capa.

Las otras dos sedes (Bilbao y O´Donell) y los usuarios del edificio principal constituyen la capa de acceso.

3.4 Modelo de referencia OSI

Los usuarios deben asegurarse que sus datos se entreguen y reciban de manera adecuada, de ahí la necesidad de que dichos datos tengan un formato claro y eficiente, verificando los servicios que involucra, tales como protocolos de traducción de formatos, códigos y sintaxis de los lenguajes, entre una computadora emisora y una receptora.

Es aquí donde el Modelo de Referencia de Interconexión de Sistemas Abiertos (Open System Interconnection u OSI) cobra la importancia que merece, al permitir que diferentes sistemas se interconecten e interoperen, gracias a reglas preestablecidas que deben ir cumpliéndose nivel a nivel para su total desempeño, logrando el concepto de Internetworking.

El modelo de referencia OSI proporciona una forma de entender cómo opera un internetworking de redes y sirve de guía o marco de trabajo para implementar estándares de red, dispositivos y esquemas de internetworking. Las ventajas que ofrece este modelo estructurado en capas son:

- Separar la compleja operación de internetworking en elementos más simples.
- Permitir el diseño y desarrollo de funciones modulares.
- Posibilidad de definir interfaces estándar para compatibilidad “plug-and-play” e integración multifabricante.

El modelo de referencia OSI consta de siete capas. Las cuatro capas de nivel inferior definen rutas para que los puestos finales puedan conectarse unos con otros y poder intercambiar datos. Las tres capas superiores definen cómo han de comunicarse las aplicaciones de las estaciones finales entre ellas y con los usuarios.

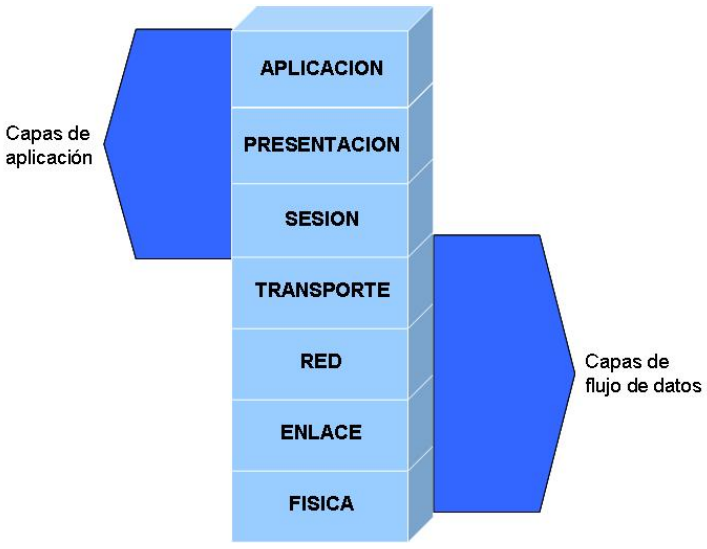


Figura 3-3 Modelo de referencia OSI

3.4.1 Capas Superiores

Las tres capas superiores del modelo de referencia OSI se denominan habitualmente capas de aplicación. Estas capas están relacionadas con la interfaz de usuario, formatos y acceso a las aplicaciones.

- **Capa de aplicación**. Es la capa de nivel superior del modelo. Aquí, el usuario o la aplicación dialoga con los protocolos para acceder a la red. Por ejemplo, se accede a un procesador de textos por el servicio de transferencia de archivos de esta capa.

- **Capa de presentación.** La capa de presentación proporciona diversas funciones de conversión y codificación que se aplican a los datos de la capa de aplicación. Estas funciones aseguran que los datos enviados desde la capa de aplicación de un sistema podrán ser leídos por la capa de aplicación de otro sistema. Un ejemplo de funciones de codificación sería el cifrado de datos una vez que éstos salen de una aplicación. Otro ejemplo podrían ser los formatos de imágenes jpeg y gif que se muestran en páginas WEB. Este formato asegura que todos los navegadores WEB podrán mostrar las imágenes, con independencia del sistema operativo utilizado.

- **Capa de sesión**. La capa de sesión es la responsable de establecer, administrar y finalizar las sesiones de comunicaciones entre entidades de la capa de presentación. La comunicación en esta capa consiste en peticiones de servicios y respuestas entre aplicaciones ubicadas en diferentes dispositivos. Un ejemplo de este tipo de coordinación podría ser el que tiene lugar entre un servidor y un cliente de base de datos.

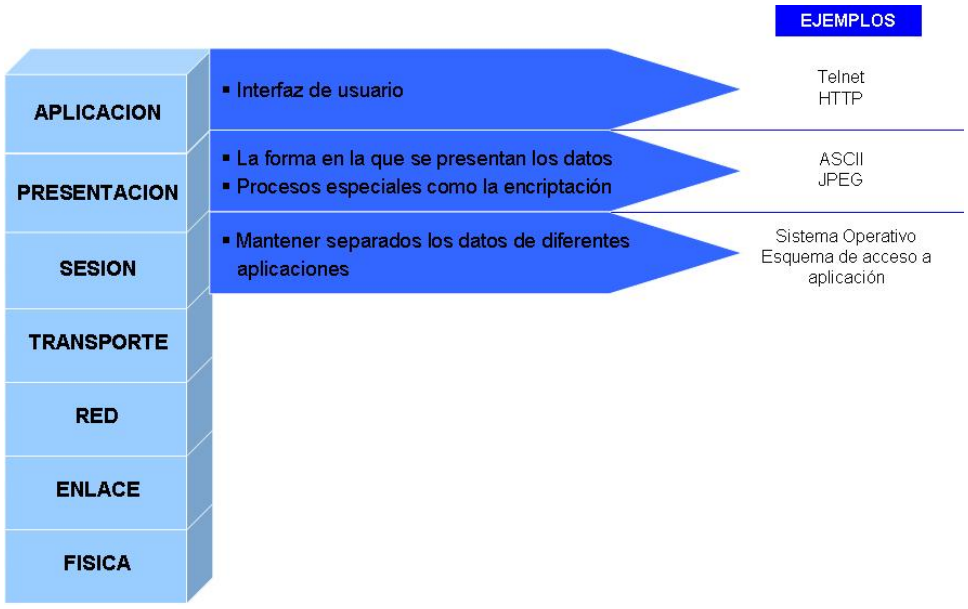


Figura 3-4 Modelo OSI. Capas Superiores

3.4.2 Capas Inferiores

Las cuatro capas inferiores del modelo de referencia OSI son las responsables de definir el modo en el que los datos se transmiten por un medio físico, a través de dispositivos de red, hasta la estación final y finalmente a su correspondiente aplicación.

- **Capa de transporte**. En este nivel se garantiza la calidad de la comunicación, ya que asegura la integridad de los datos. Es aquí donde se realizan las retransmisiones cuando la información fue corrompida o porque alguna trama del nivel 2 detectó errores en el formato y se requiere volver a enviar el paquete o datagrama. El nivel de transporte notifica a las capas superiores si se está logrando la calidad requerida. Este nivel utiliza reconocimientos, números de secuencia y control de flujo. Los protocolos TCP (Transmission Control Protocol) y UDP (User Datagram Protocol) son característicos del nivel del transporte del modelo OSI. El primero de ellos es fiable u orientado a conexión, mientras que UDP es no fiable, o independiente de la conexión.

  En la capa 4 operan los switch de capa 4 y los firewalls, que filtran la información en base al puerto donde se realiza las conexiones.

- **Capa de red.** El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan routers. Adicionalmente la capa de red lleva un control de la congestión de red, que es el fenómeno que se produce cuando la saturación de un nodo tira abajo toda la red En este nivel se realiza también el direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final.

  En la capa de red principalmente operan los routers o los switches de capa 3. Estos dispositivos proporcionan rutas para todas las redes del internetworking. Los switches de capa 3 aunque trabajan en esta capa, en determinados casos, pueden actuar como switch de nivel 2. Los firewalls también pueden actuar sobre la capa de red para descartar direcciones de máquinas

- **Capa de enlace.** Cualquier medio de transmisión debe ser capaz de proporcionar una transmisión sin errores, es decir, un tránsito de datos fiable a través de un enlace físico. Debe crear y reconocer los límites de las tramas, así como resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas. También puede incluir algún mecanismo de regulación del tráfico que evite la saturación de un receptor que sea más lento que el emisor. La capa de enlace de datos se ocupa del direccionamiento

físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

En la capa 2 realizan su función los switches, que dividen la red en segmentos independientes, con pocos usuarios por segmento. Los puntos de acceso y puentes inalámbricos también trabajan en esta capa

- **Capa física.** La capa física define el tipo de medio, tipo de conector y tipo de señalización. Especifica los requisitos eléctricos, mecánicos, procedimentales y funcionales para activar, mantener y desactivar el vínculo físico entre sistemas finales, así como características tales como niveles de voltaje, tasas de transferencia de datos, distancias máximas de transmisión y conectores físicos.

  En la capa 1, capa física, operan los Hubs. Este elemento transmite paquetes y actúa como concentrador para otros dispositivos de red.

Figura 3- 5 Modelo OSI. Capas Inferiores

3.4.3 Dispositivos utilizados en el IATE

Cada dispositivo de red opera en una capa diferente del modelo OSI. Sin embargo, algunos de ellos trabajan a nivel de varias capas, dependiendo de la función que se le asigne.

En el IATE se requieren dispositivos tales como firewall, routers, switches de capa 3, switches, y puentes inalámbricos, sin embargo, los Hubs serán eliminados de la nueva infraestructura de

red. La siguiente figura agrupa dichos dispositivos según la capa del modelo OSI en la que operan.

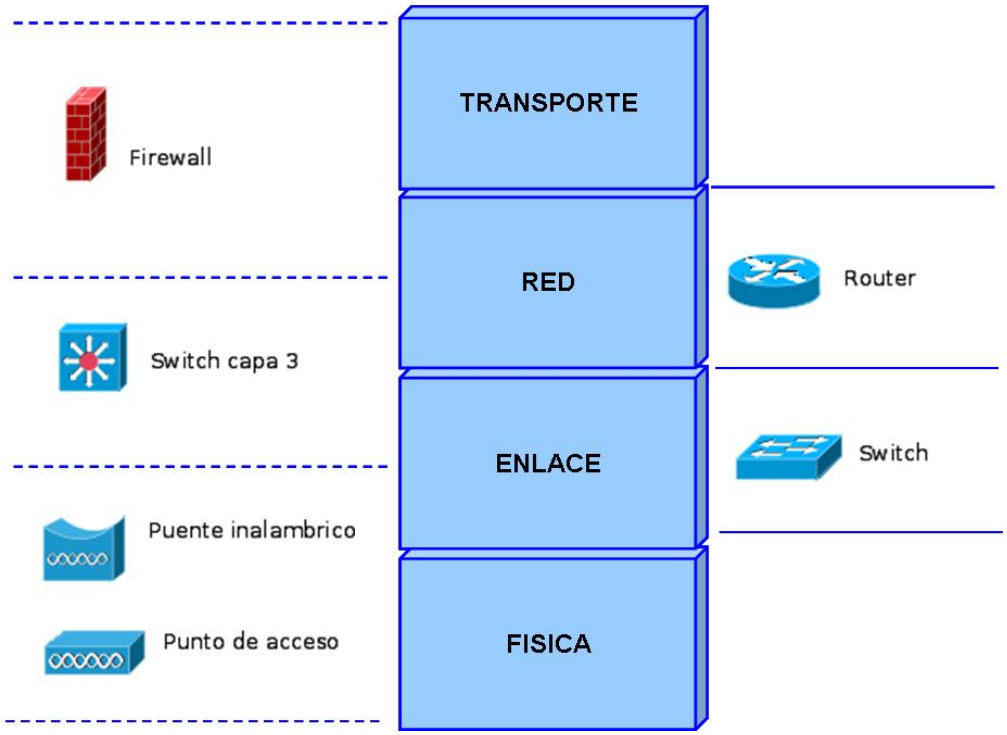


Figura 3- 6 Agrupación de dispositivos según capas del modelo OSI

3.5 Arquitectura Lógica

El diseño lógico es el proceso de construir un esquema de la información que utiliza la empresa. En esta etapa, se transforma el esquema conceptual en un esquema lógico, como puede ser el modelo jerárquico.

El esquema lógico es una fuente de información para el diseño físico. Y lo que es más, juega un papel importante durante la etapa de mantenimiento del sistema. El diseño lógico es una etapa clave para conseguir un sistema que funcione correctamente y mantener unas prestaciones aceptables. Además teniendo en cuenta que la capacidad de ajustarse a futuros cambios es un sello que identifica a los buenos diseños, es fundamental dedicar el tiempo y las energías necesarias para producir el mejor esquema que sea posible.

A continuación, la Figura 3-7 muestra la arquitectura lógica para la red del IATE.

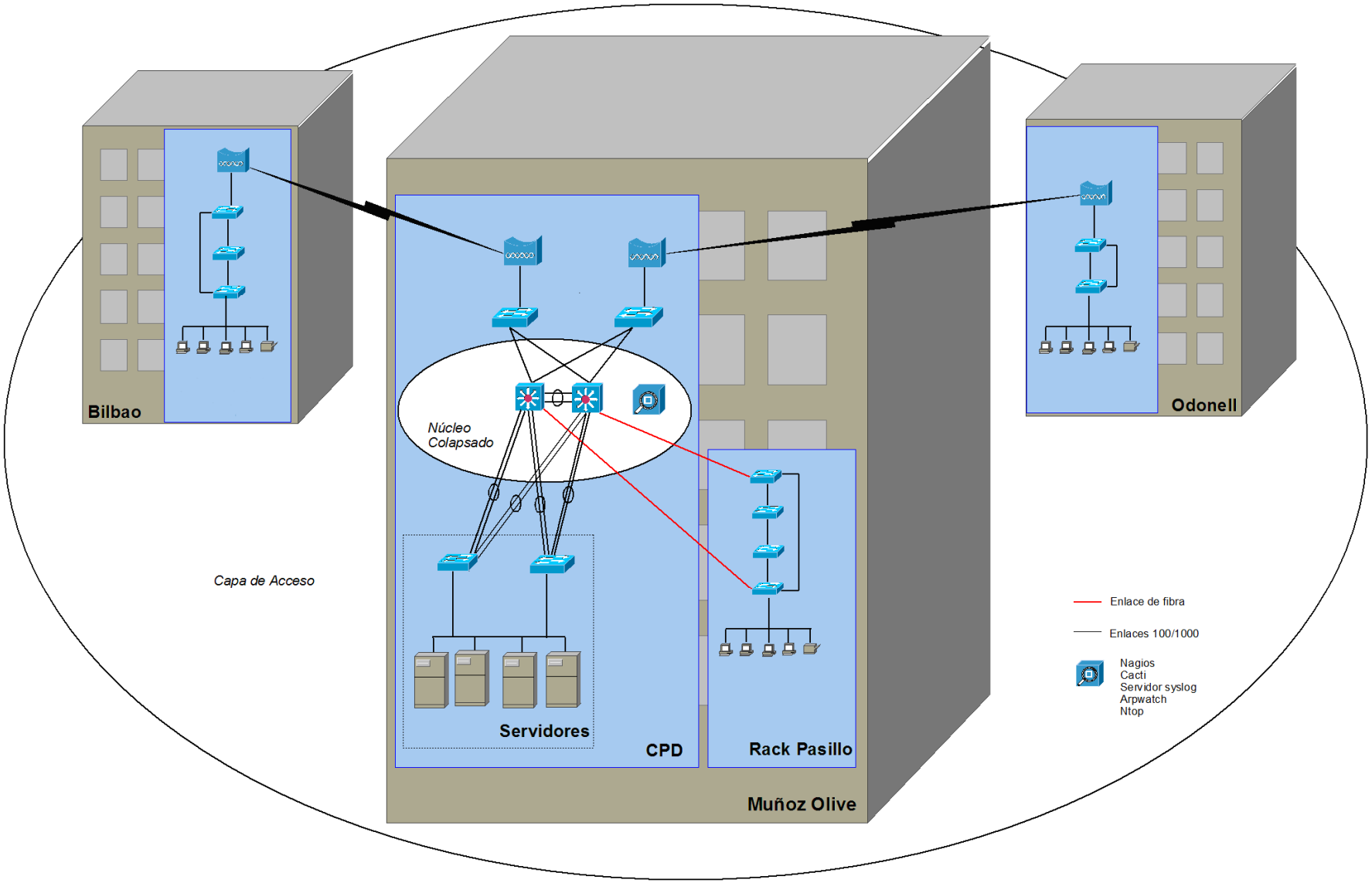


Figura 3-7 Arquitectura Lógica para el IATE

3.6 Arquitectura Física

3.6.1 Tecnologías de interconexión

Existen diversas tecnologías disponibles para interconectar dispositivos en la red. Algunas de las más comunes se enumeran a continuación.

- **Fast Ethernet (100 Mbps):** Esta especificación de LAN (IEEE 802.3u) opera a 100 Mbps a través de cable de par trenzado, aumentando la velocidad de Ethernet de 10 a 100 Mbps, solo con mínimos cambios en la estructura de cableado existente.

- **Gigabit Ethernet:** Es una extensión del Ethernet estándar IEEE 802.3 que aumenta la velocidad diez veces más que el Fast Ethernet, es decir, a 1000 Mbps o 1 Gbps. La norma IEEE 802.3z especifica operaciones sobre fibra óptica, y el estándar IEEE 802.3ab especifica operaciones a través de cable de par trenzado.

- **10-Gigabit Ethernet:** Fue formalmente ratificado como estándar IEEE 802.3 Ethernet en Junio de 2002. Esta tecnología es el siguiente paso para escalar el rendimiento y la funcionalidad de una empresa. Con el despliegue cada vez más frecuente de Gigabit Ethernet, 10-Gigabit se convierte en la norma para los enlaces ascendentes.

Los dispositivos de Cisco permiten la agregación de puertos, conocida en la terminología de Cisco como **EtherChannel.** Esta característica permite la agregación de enlaces de ancho de banda sobre enlaces de capa 2 entre dos switches Cisco Catalyst. EtherChannel agrupa varios enlaces Ethernet en un único puerto lógico, proporcionando un ancho de banda agregado de hasta 16 veces la capacidad máxima del enlace (full-duplex). Por ejemplo, agrupando 8 enlaces Fast Ethernet de 100 Mbps cada uno, se puede lograr una capacidad de hasta 1600 Mbps en full-duplex, o hasta 16 Gbps si son 8 enlaces Gigabit. Todas las interfaces en cada paquete EtherChannel deben estar configuradas con velocidad similar, en modo duplex, y pertenecer a la VLAN.

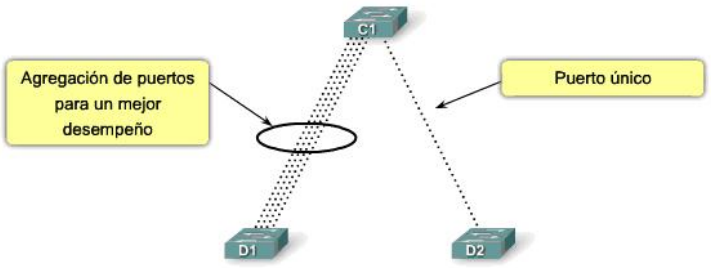
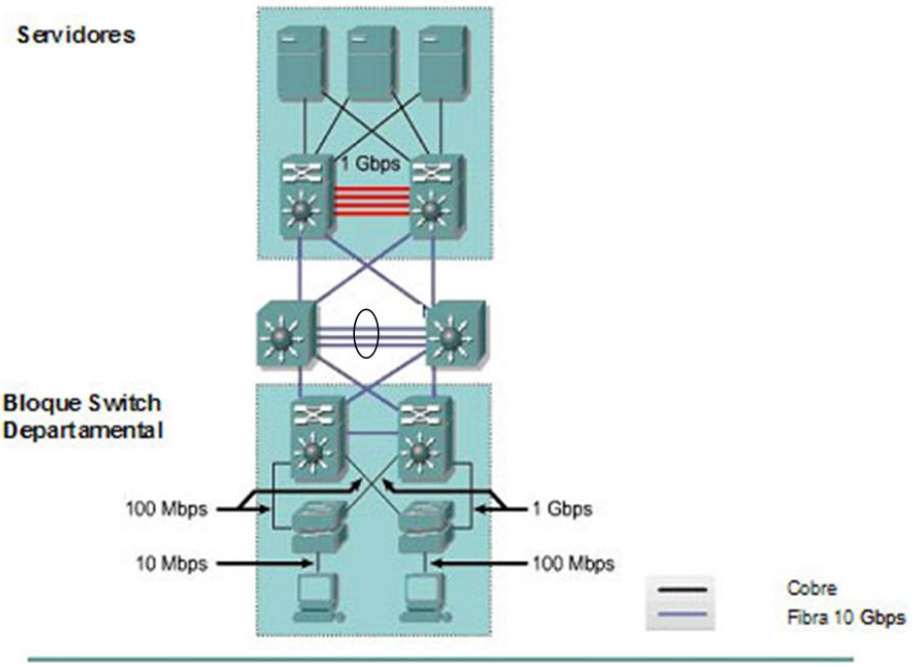


Figura 3-8 Agregación de puertos

La tecnología de interconexión seleccionada dependerá de la cantidad de tráfico que deba soportar el enlace. Probablemente se usará una mezcla entre cableado de cobre y fibra óptica, basado en la distancia, requisitos de inmunidad al ruido, seguridad y otros requisitos corporativos.



TECNOLOGÍA	USO
Fast Ethernet	Se usa frecuentemente para conectar dispositivos de usuarios finales al switch de la capa de acceso.
Gigabit Ethernet	Acceso tanto a los switches de distribución como a los servidores.
10-Gigabit Ethernet	Enlaces de alta velocidad entre switches del backbone.

Figura 3-9 Tipos/Usos de tecnologías de interconexión.

Hay cuatro objetivos en el diseño de cualquier red de alto rendimiento: seguridad, disponibilidad, escalabilidad y mantenimiento. El modelo, cuando se implementa apropiadamente, satisface estos objetivos.

Para llevar a cabo la migración de la infraestructura de red actual a la futura red gestionable, se han considerado las siguientes decisiones en cuanto a equipamiento y cableado.

1. Reemplazar hubs y switches no gestionables por nuevos switch en la capa de acceso, cuya velocidad de puerto sea la apropiada y planificando con un 30% de crecimiento el número de puertos necesarios.

2. Si los switches de la capa de acceso tiene problemas de ancho de banda para conducir todo el tráfico a los switch de distribución, crear enlaces EtherChannel para agregar el ancho de banda que sea necesario.

3. En la construcción de la capa de distribución, seleccionar switches con el rendimiento adecuado para soportar la carga de la capa de acceso. Estos dispositivos deben ser switches multicapas (Layer 2/Layer 3) que soporten enrutamiento entre las VLANs del grupo de trabajo y los recursos de red.

4. El equipamiento del núcleo debe soportar comunicaciones de alta velocidad de datos.

3.6.2 Descripción del equipamiento

Con respecto a la electrónica de red para la LAN del IATE, básicamente la mayor inversión se realizará en la compra de switches. Entre los factores a considerar a la hora de elegir los switches para la capa de acceso se incluyen los siguientes:

- Spanning Tree: Proporciona una arquitectura libre de bucles. Se recomienda soportar "rapid spanning tree"

- Características de seguridad en capa 2, CISF (Cisco Integrated Security Features), tales como seguridad en puerto, DAI (Dinamic ARP inspection), Address Resolution Protocol (ARP) Spoofing, Media Access Control (MAC) Flooding, Dynamic Host Configuration Protocol (DHCP) Snooping, VLAN Hooping, etc.

- Soporte para VLANs, de forma que los empleados estén conectados por departamentos, equipos de proyecto o aplicaciones, en lugar de por criterios físicos o geográficos.

- Soporte para análisis de puertos, SPAN (Support for Switched Por Analyzer)

- Soporte para mantenimiento por SNMP (Simple Network Management Protocol).

- Velocidad de reenvío. Define las capacidades de procesamiento mediante la estimación de la cantidad de datos que el switch puede procesar por segundo. Los switches de la capa de acceso presentan velocidades inferiores que los de la capa núcleo.

- Agregado de ancho de banda. Ayuda a reducir los cuellos de botella al permitir la unión de varios enlaces Ethernet en un único puerto lógico. Con el agregado de enlaces múltiples de 10 Gigabit Ethernet en algunos switches de la capa empresarial, es posible

lograr tasas de rendimiento muy altas. Como se vio anteriormente, Cisco utiliza el término EtherChannel cuando describe los puertos de switch agregados.

- Capacidades de Power-over-Ethernet (PoE), que minimizan la cantidad de cableado eléctrico necesario para los dispositivos de red y permiten implementar nuevas funcionalidades como voz y tecnología inalámbrica sin necesidad de cableado nuevo.

- Capacidades de autenticación 802.1x

Tras el análisis realizado en el primer capítulo se llegó a la conclusión de que integrar routers y switches Cisco permite reducir el coste total de propiedad de la red (TCO) y obtener así un mayor retorno de la inversión, por lo que finalmente la marca seleccionada para el desarrollo del presente proyecto fue Cisco.

La familia Catalyst de Cisco es una completísima línea de switches de alto rendimiento diseñados para ayudar a migrar de forma sencilla una red LAN compartida tradicional a una red completamente conmutada. Ofrece un amplio espectro para aplicaciones de usuarios, desde switches para pequeños grupos de trabajo hasta switches multicapa para aplicaciones empresariales escalables en el centro de datos o en el backbone.

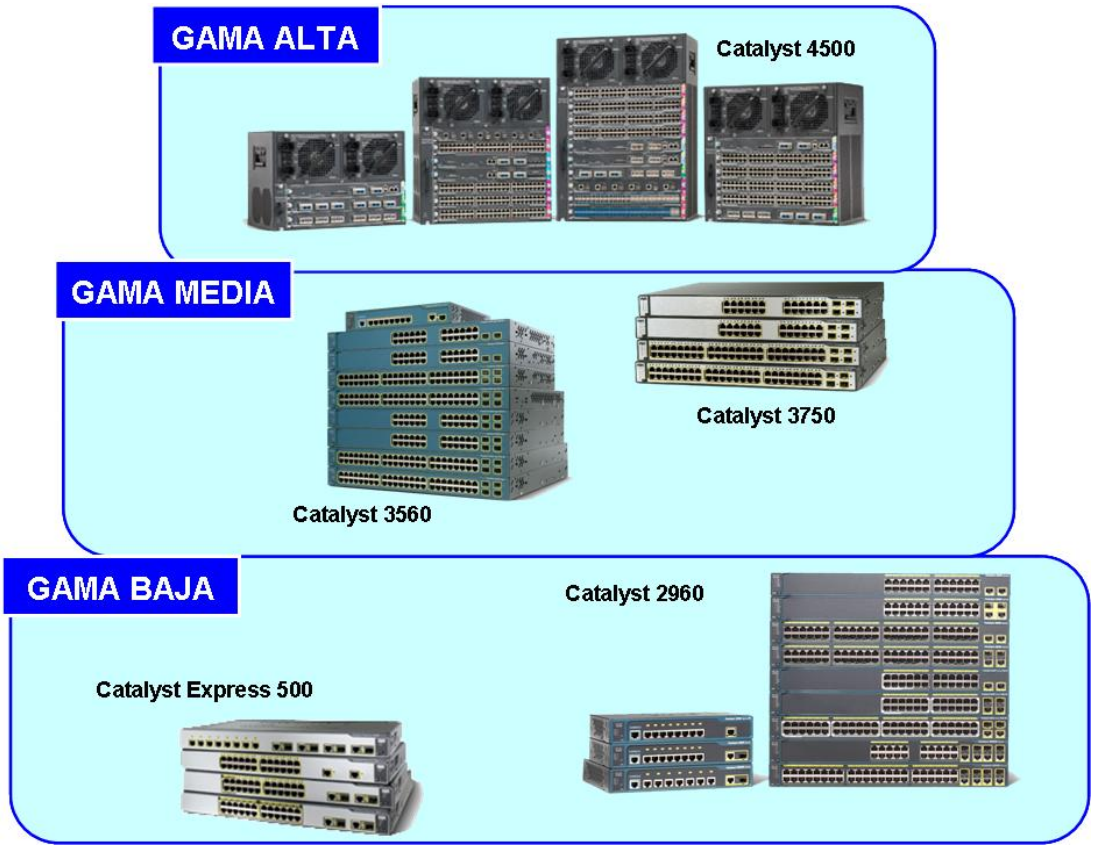


Figura 3-10 Gamas de Switches Cisco Catalyst para la capa de acceso

La Figura 3-10 muestra las alternativas que ofrece Cisco Catalyst para la capa de acceso. Todos ellos, en mayor o menor medida, soportan las características anteriormente citadas. Conforme aumenta la gama, el precio del dispositivo se incrementa considerablemente, de ahí que se descarten los de la serie 3750 y 4500. Finalmente teniendo en cuenta que en ninguna de las sedes se superan los 250 usuarios y que en estos casos, Cisco recomienda los switches de gama baja, la elección estará entre la serie Express 500 y la serie 2960.

La siguiente tabla compara las características que incluyen los switches Cisco Catalyst de la serie Express 500 y 2960. Ambos permiten crear una completa red de área local que aloje dispositivos cableados e inalámbricos, debido a que están diseñados para gestionar alrededor de 250 usuarios, por lo que facilitan la incorporación de nuevos empleados conforme crece la red.

CARACTERÍSTICAS	Cisco Catalyst Express 500	Cisco Catalyst Serie 2960
Fast Ethernet / Gigabit Ethernet	✓	✓
Soporte para comunicaciones de datos, inalámbrica y de voz	✓	✓
Capacidad para configurar VLANs	✓	✓
Capacidades de Power-over-Ethernet	✓	NO
Seguridad integrada y monitorización de red	✓	Mejoradas
Administración	WEB	WEB / Consola / Acceso Remoto
Número de usuarios soportados	20 - 250	Más de 250

Tabla 3-1 Switches de la Serie Express 500 vs. Serie 2960 (Capa de acceso)

La serie de switches de Cisco Catalyst Express solo son administrables vía WEB, dificultando realizar configuraciones mas personalizadas, mientras que los Cisco Catalyst Serie 2960 permiten tanto configuración WEB como remota o por consola. Por otro lado, la serie 2960 destaca por sus funciones de monitorización de red y solución de problemas de conectividad, así como por incorporar seguridad integrada mejorada, que permite proteger la información importante, manteniendo a los usuarios no autorizados alejados de la red y consiguiendo un funcionamiento ininterrumpido, características que la convierten en la mejor opción.

Entre los factores a considerar a la hora de elegir los switches para la capa núcleo/distribución, además de los expuestos al comienzo del apartado, se incluyen los siguientes:

- Routing
- Alta disponibilidad
- Lista de control de acceso entre VLANs (VACL)

La Figura 3-11 muestra las alternativas que ofrece Cisco Catalyst para la capa núcleo/distribución. Por la misma razón que en el caso anterior, se descarta la gama alta. Por otro lado, mientras que el switch 3560 es el más apropiado para pequeña y medianas empresas, los de gama media en adelante son usados para proveedores de servicios. Por este motivo, y una vez más tomando como criterio el número de usuarios que van a acceder a la red, la gama baja se considera la mejor opción para el caso que nos ocupa.

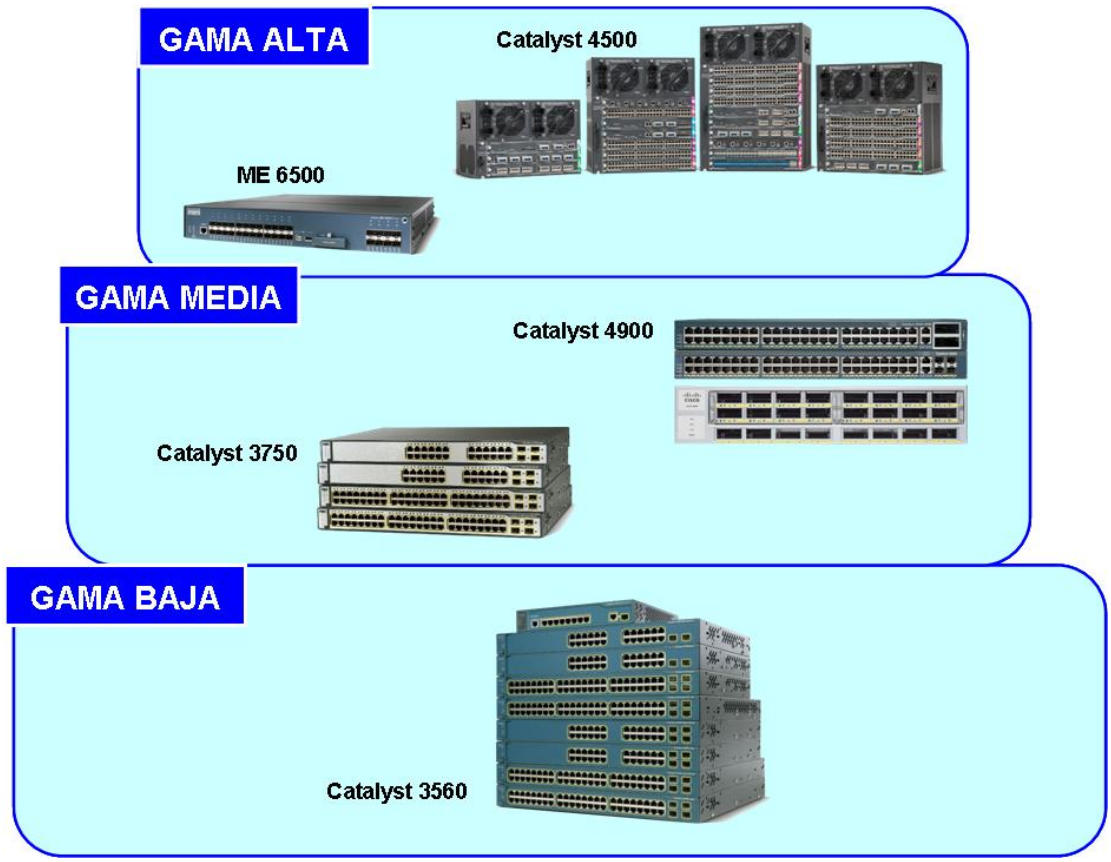


Figura 3-11 Gamas de Switches Cisco Catalyst para la capa distribución y núcleo

Además de las características descritas en la Tabla 3-1 para los switches de la serie 2960, los switches Cisco Catalyst de la serie 3560 poseen las siguientes:

- Conmutación Layer 3 y Layer 2
- Enrutamiento IP
- Instancia de la tabla de enrutamiento (Route Forwarding-Lite o VRF-Lite)

La Tabla 3-2 presenta a modo de resumen algunas de las características técnicas más importantes para los switches Cisco Catalyst de la serie 3560 y de la serie 2960, concretamente para los 2960 y 2960G (Gigabyte). Este ultimo seleccionado para los servidores de la capa de acceso por proporcionar un mejor rendimiento en el acceso a los mismos. Al mismo tiempo la tabla refleja el número de dispositivos de cada tipo que deberán ser adquiridos por parte del IATE para el desempeño del presente proyecto. La cantidad de cada tipo de dispositivo adquirida se ha sobredimensionado en 1 unidad con el fin de disponer de equipos de repuesto.

	CAPA DE ACCESO		CAPA NÚCLEO
ELEMENTO DE COMUNICACIÓN	**2960/2960S**	**2960 G**	**3560**
Capas OSI admitidas	Capa 2	Capa 2	Capa 2 y 3
Fast Ethernet	24 puertos	0	0
Velocidad de reenvío	8.8 a 24 Gb/s	32 Gb/s	32 Gb/s a 128 Gb/
Gigabit Ethernet	2 puertos/4 puertos	24 puertos	26 puertos
Protocolo	Spanning-Tree IEEE 802.1w	Spanning-Tree IEEE 802.1w	Spanning-Tree IEEE 802.1w
Unidades requeridas para el IATE	**15 / 3**	**3**	**3**

Tabla 3-2 Sumario de especificaciones Técnicas para los switches seleccionados.

Además del número de switches indicado en la tabla anterior son necesarios:

- 4 puentes inalámbricos del tipo Bridge Linksys

Para una información más detallada, las especificaciones técnicas de estos dispositivos se adjuntan como información adicional en el anexo B, Hardware Empleado.

A continuación, la Figura 3-12 y la Figura 3-13 muestran la arquitectura física para la red del IATE. Como se puede observar en la Figura 3-13 se ha contratado una línea de backup de 10Mbps a la red corporativa, para que en caso de fallo de la línea principal no se produzca corte del servicio. La administración y gestión del router principal y de backup no son objetos de este proyecto, su responsabilidad recae en Red Corporativa, que es el proveedor de servicios para el IATE, por lo que solo nos proporcionan la IP HSRP de sus routers.

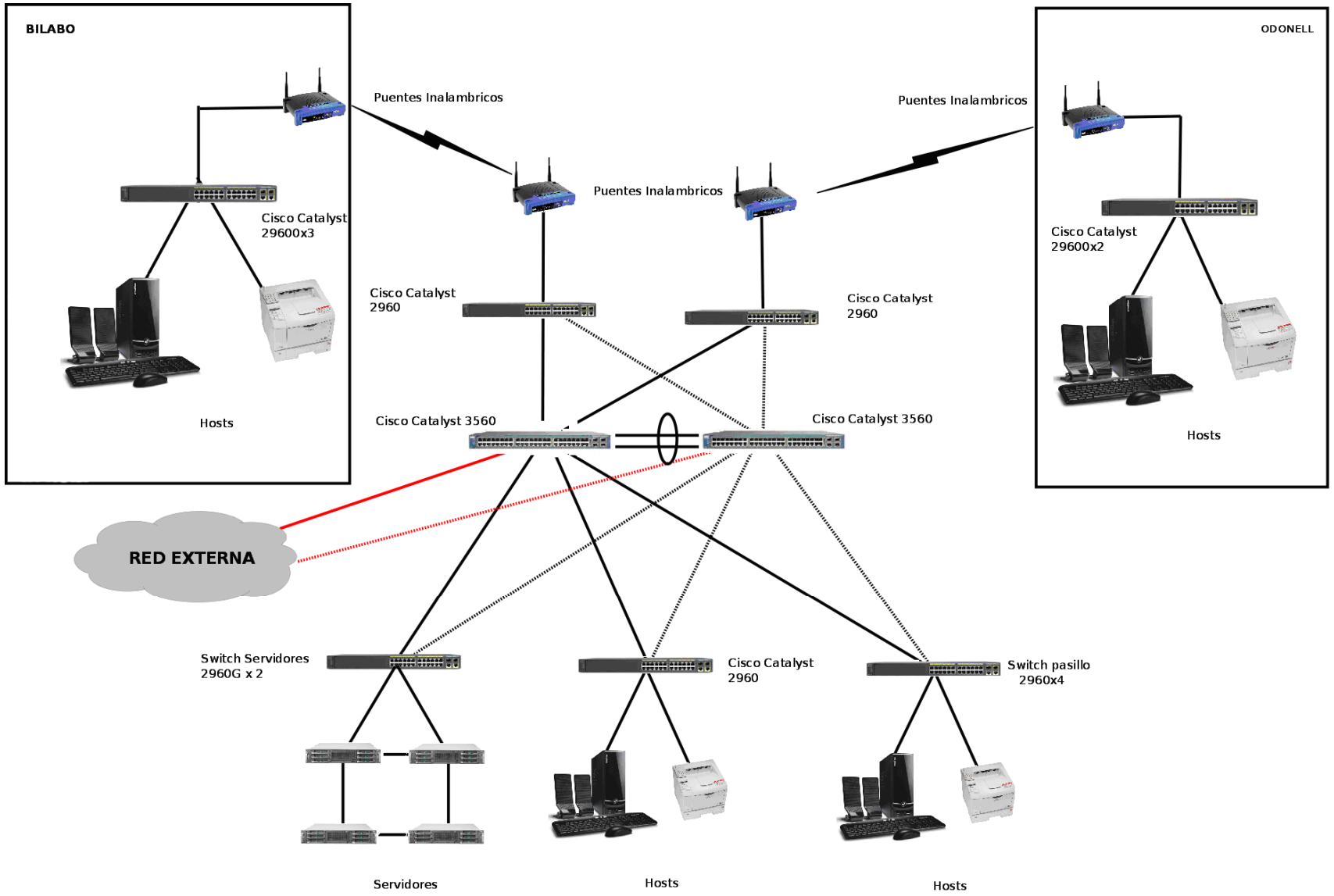


Figura 3-12 Arquitectura Física para el IATE

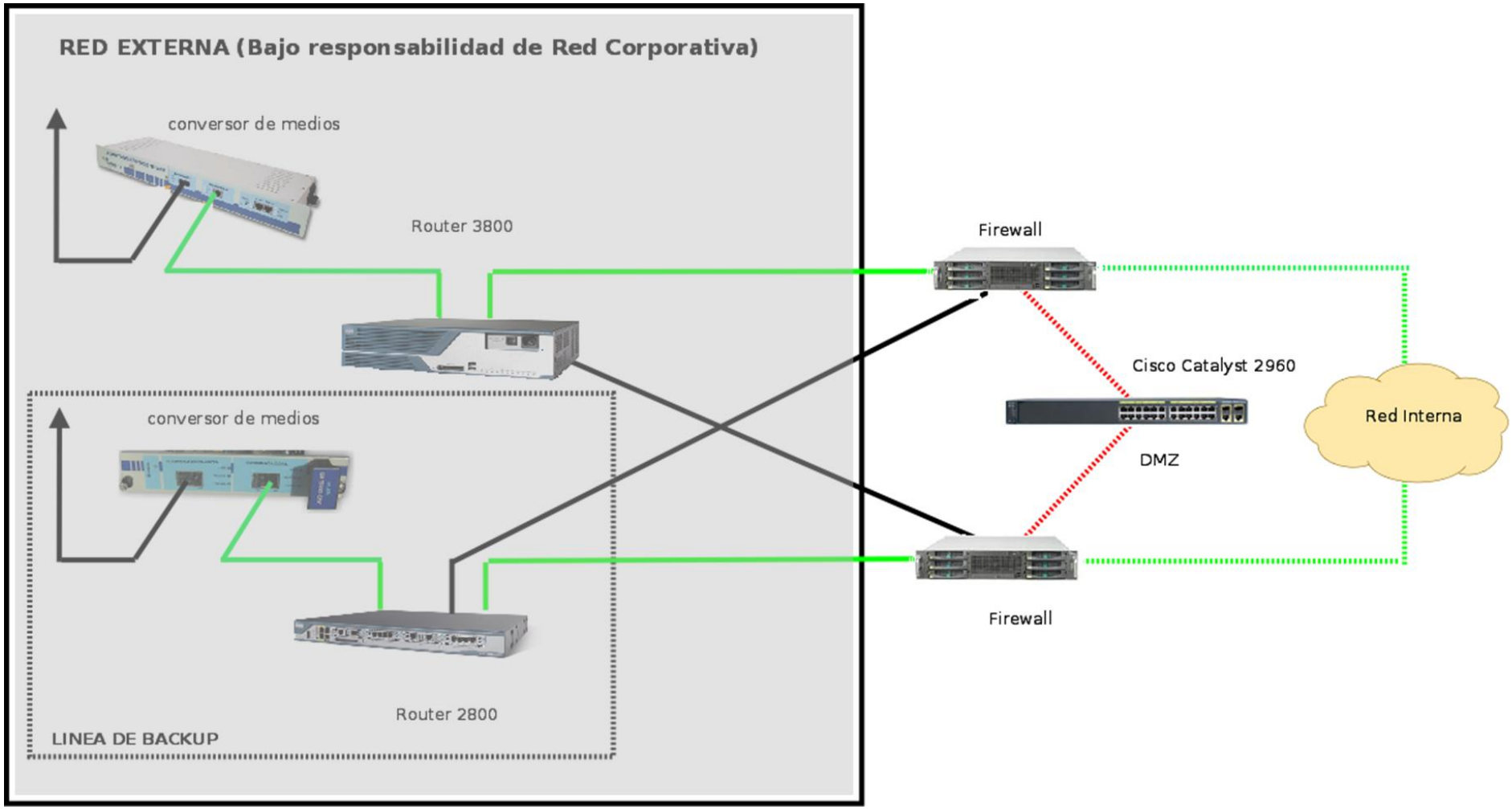


Figura 3-13 Arquitectura Física para la Red Externa

3.6.3 Localización de los equipos

El diseño de la red involucra la localización de cada uno de sus elementos. Es quizás una de las partes más importantes del proceso, puesto que una buena documentación de la red permite obtener rápidamente información sobre un dispositivo determinado, además de servir como referencia para analizar, comparar y verificar el estado de la red.

La documentación de la red debe incluir la configuración, un diagrama de la topología de la red e información tabulada acerca de cada componente. Dicha información debe encontrarse en un solo lugar, ya sea impresa o en la red, para facilitar su control y actualización. Lo recomendable es que esté accesible desde cualquier punto de la red y en cualquier momento, sin embargo, una copia de la documentación también debe mantenerse en una ubicación segura fuera del lugar habitual.

Es evidente que cualquier actualización en la documentación de red debe seguir un proceso de normalización y estar bajo control de versiones, de tal forma que se localicen fácilmente los cambios y se tenga perfecto conocimiento de la configuración de cada componente. Por tanto, para llevar a cabo esta labor, se requiere establecer una metodología y la asignación de responsabilidades en cuanto a la modificación y distribución de la documentación de red una vez debidamente actualizada.

En el diagrama de la topología se debe mostrar cómo se conecta cada dispositivo en la red, mientras que también se detallan los aspectos de su arquitectura lógica. Cada dispositivo de red debe estar representado con notación coherente o un símbolo gráfico, al mismo tiempo que cada conexión física y lógica debe estar representada mediante una línea simple o algún símbolo apropiado.

Las tablas de configuración deben recopilar toda la información relevante asociada a cada dispositivo, habitualmente, tienen una estructura similar a las mostradas a continuación.

Nombre y Modelo del Catalyst IP Administración	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN	Información de la localización

Tabla 3-3 Documentación de la red – Información relevante para los switches Catalyst

Router, Modelo y numero de Serie	Interface	Dirección MAC	IP / Mascara de Subred	Protocolo de Enrutamiento	Información de la localización	Version IOS	Número de serie

Tabla 3-4 Documentación de la red - Información relevante para los Routers

Nombre del dispositivo	Sistema operativo	IP/Mascara de subred	Estática/Dinámica	VLAN

Tabla 3-5 Documentación de la red - Información relevante para las estaciones finales

A continuación se muestra un diagrama de flujo donde se ilustran los pasos a seguir a la hora de documentar un dispositivo de red.

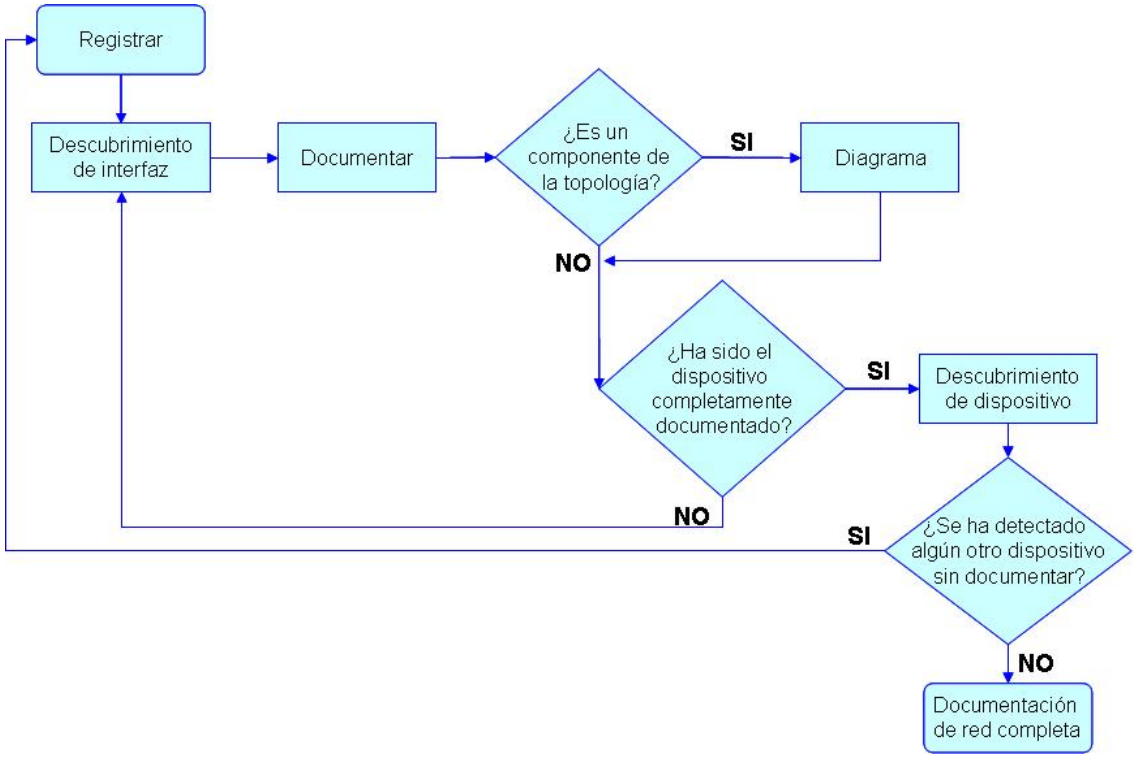


Figura 3-14 Diagrama de flujo a seguir para documentar un dispositivo de red

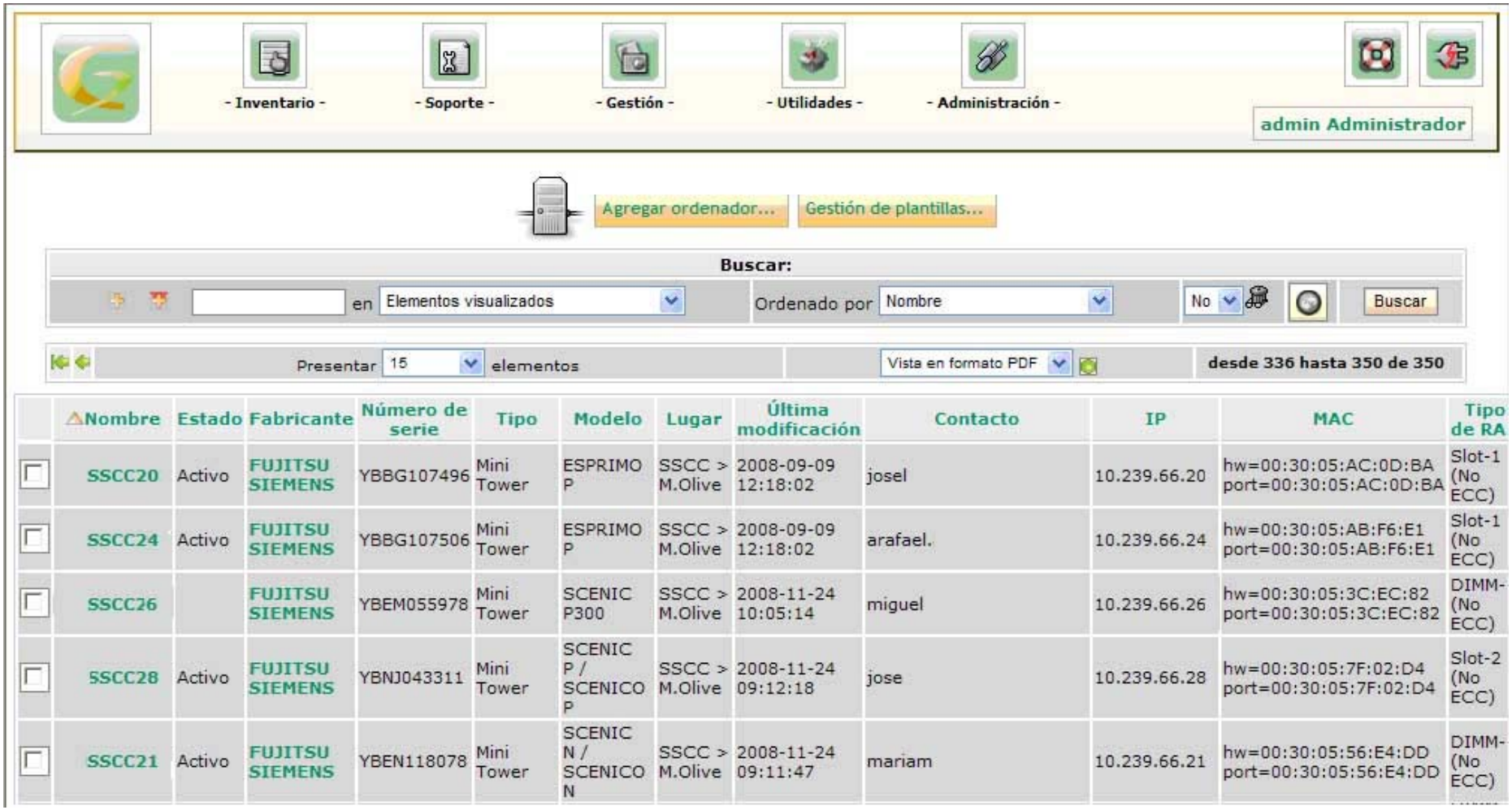
- **Paso 1 -** Registrar el nuevo dispositivo
- **Paso 2 -** Descubrimiento de interfaz. Recopilar información relevante sobre el dispositivo
- **Paso 3 -** Documentar dicha información en las tablas de configuración. Si se trata también de un componente del diagrama de la topología, ejecutar el paso 4. Si toda la información relevante sobre el dispositivo ha sido documentada, saltar el paso 4 y pasar al 5.
- **Paso 4 -** Transferir cualquier información sobre el dispositivo desde la tabla de configuración de la red que corresponda al diagrama de topología. Una vez finalizado, si toda la información relevante sobre el dispositivo ha sido documentada, ir al paso 5. En caso contrario, volver al paso 2.
- **Paso 5 -** Determinar si cualquier dispositivo vecino está sin documentar. En caso afirmativo, volver al paso 1. En otro caso, finalizar el proceso y considerar completa la documentación de la red.

Para el caso del IATE, los diagramas de topologías son los mostrados en la Figura 3-7, Figura 3-12 y Figura 3-13 del presente documento. En cuanto a las tablas, debido a la extensión de las mismas, se han incluido en el anexo C, Documentación de la red.

Por otra parte, como complemento a la documentación de red, además se puede confeccionar un inventario de equipos, que recopila información del hardware y software del equipo. Para ello se dispone de herramientas de software libre como Open Computer and Software Inventory Next Generation (OCS) y Gestionnaire Libre de Parc Informatique (GLPI).

OCS presenta vía WEB información sobre el hardware y software de la empresa, obtenida mediante un agente instalado en los equipos. Por su parte, GLPI facilita la administración de recursos informáticos y de los historiales de las diferentes labores de mantenimiento y procedimientos llevados a cabo sobre esos recursos informáticos. Una excelente idea es integrar GLPI y OCS conjuntamente.

Figura 3-15 Menú de opciones de la herramienta GLPI



Nombre	Estado	Fabricante	Número de serie	Tipo	Modelo	Lugar	Última modificación	Contacto	IP	MAC	Tipo de RA
SSCC20	Activo	FUJITSU SIEMENS	YBBG107496	Mini Tower	ESPRIMO P	SSCC > M.Olive	2008-09-09 12:18:02	josel	10.239.66.20	hw=00:30:05:AC:0D:BA port=00:30:05:AC:0D:BA	Slot-1 (No ECC)
SSCC24	Activo	FUJITSU SIEMENS	YBBG107506	Mini Tower	ESPRIMO P	SSCC > M.Olive	2008-09-09 12:18:02	arafael.	10.239.66.24	hw=00:30:05:AB:F6:E1 port=00:30:05:AB:F6:E1	Slot-1 (No ECC)
SSCC26		FUJITSU SIEMENS	YBEM055978	Mini Tower	SCENIC P300	SSCC > M.Olive	2008-11-24 10:05:14	miguel	10.239.66.26	hw=00:30:05:3C:EC:82 port=00:30:05:3C:EC:82	DIMM- (No ECC)
SSCC28	Activo	FUJITSU SIEMENS	YBNJ043311	Mini Tower	SCENIC P / SCENICO P	SSCC > M.Olive	2008-11-24 09:12:18	jose	10.239.66.28	hw=00:30:05:7F:02:D4 port=00:30:05:7F:02:D4	Slot-2 (No ECC)
SSCC21	Activo	FUJITSU SIEMENS	YBEN118078	Mini Tower	SCENIC N / SCENICO N	SSCC > M.Olive	2008-11-24 09:11:47	mariam	10.239.66.21	hw=00:30:05:56:E4:DD port=00:30:05:56:E4:DD	DIMM- (No ECC)

Figura 3-16 Inventariado de equipos con la herramienta GLPI

Tag	Último inventario	Computador	Nombre usuario	Sistema Operativo	RAM(MB)	CPU(MHz)
NA	26/02/2010 08:11:13	SSCC124	francisca	Microsoft Windows 2000 Professional	512	3192
NA	08/03/2010 09:48:30	SSCC155	elvira	Microsoft Windows XP Professional	1024	3192
NA	28/12/2009 12:39:17	SSCC147	pablo	Microsoft Windows 2000 Professional	512	3192
NA	08/03/2010 09:11:58	SSCC157	alberto	Microsoft Windows 2000 Professional	512	3192
NA	08/03/2010 09:07:07	SSCC164	daniel.g	Microsoft Windows XP Professional	2048	3192
NA	08/02/2010 09:39:03	SSCC121	maria	Microsoft Windows XP Professional	2048	3192
NA	08/02/2010 13:27:23	SSCC122	emilioj.romero	Microsoft Windows XP Professional	2048	2394
NA	11/02/2009 13:17:14	SSCC151	josei.g	Microsoft Windows XP Professional	1024	1197
NA	04/01/2010 12:12:27	PORIAJ16	emilioj.romero.ext	Microsoft Windows XP Professional	3033	2527
NA	04/02/2010 13:10:49	PRUEBAS	emilioj.romero.ext	Microsoft Windows XP Professional	1024	1995

Figura 3-17 Inventariado de equipos con la herramienta OCS

3.7 Direccionamiento

Las direcciones IP pueden ser públicas y privadas. El direccionamiento privado está reservado para el uso interno dentro de la compañía, no es válido para Internet, y debe ser mapeado a un direccionamiento público registrado, que será el que proporcionará conexión con el exterior.

A medida que las redes crecen, aumentando el número de segmentos, se necesitan mas direcciones de red (IP), ya que cada segmento requiere un número propio. El Subnetting permite incrementar el número de redes disponibles sin solicitar una nueva dirección IP. El documento RFC 1918 define el direccionamiento privado según la tabla mostrada en la siguiente figura.

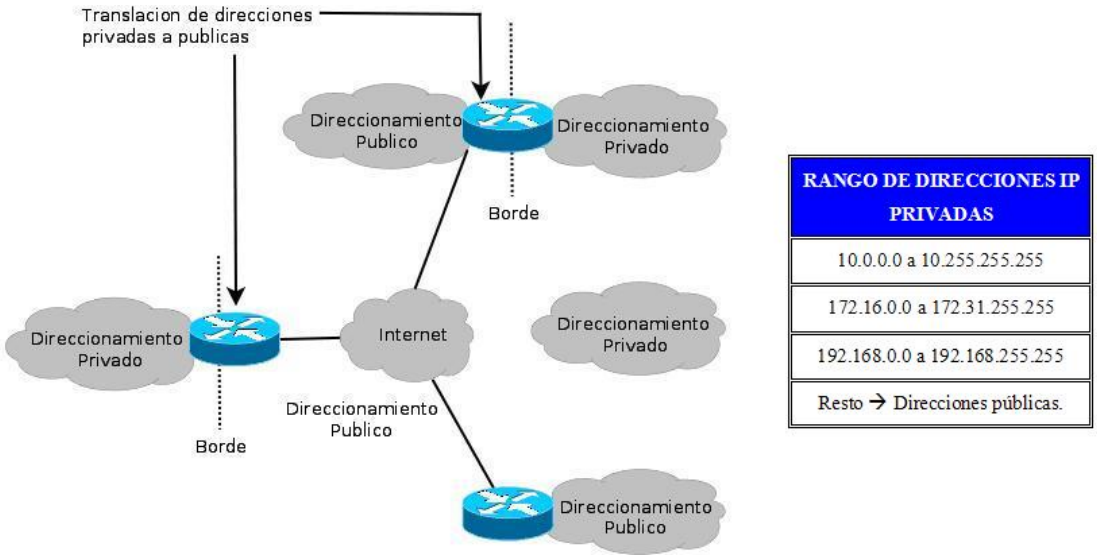


Figura 3-18 Direcciones IP públicas y privadas

Si un dispositivo de una red privada necesita comunicarse con otro dispositivo de otra red externa es necesario que el dispositivo de la red privada cuente con una puerta de enlace con una dirección IP pública. De esta manera podrá alcanzar el dispositivo externo que se encuentra fuera de la red privada, y así establecer comunicación. El router situado en la red privada podrá tener acceso a esta puerta de enlace hacia la red privada, actuando como interfaz entre la red privada y la pública. Típicamente, esta puerta de enlace será un dispositivo de traducción de dirección de red, Network Address Translation (NAT) o Port Address Translation (PAT).

Una pasarela NAT cambia la dirección origen en cada paquete de salida y, dependiendo del método, también el puerto origen para que sea único. Estas traducciones de dirección se almacenan en una tabla, para recordar qué dirección y puerto le corresponde a cada dispositivo cliente y así saber donde deben regresar los paquetes de respuesta. Si un paquete que intenta

ingresar a la red interna no existe en la tabla de traducciones, entonces es descartado. NAT tiene muchas formas de funcionamiento, entre las que destacan:

- **Estático**. Es un tipo de NAT en el que una dirección IP pública se traduce a una dirección IP privada, y donde esa dirección pública es siempre la misma. Esto le permite por ejemplo a un host, como por ejemplo un servidor Web, el tener una dirección IP de red privada pero aún así ser visible en Internet.

- **Dinámico.** Es un tipo de NAT en la que una dirección IP privada se mapea a una IP pública basándose en una tabla de direcciones de IP registradas (públicas). Normalmente, el router NAT mantendrá una tabla de direcciones IP registradas, y cuando una IP privada requiera acceso a Internet, el router elegirá una dirección IP de la tabla que no esté siendo usada por otra IP privada. Esto permite aumentar la seguridad de una red dado que enmascara la configuración interna de una red privada, lo que dificulta a los hosts externos de la red el poder ingresar a ésta. Para este método se requiere que todos los hosts de la red privada que deseen conectarse a la red pública posean al menos una IP pública asociada.

- **Sobrecarga o Port Address Translation (PAT).** La forma más utilizada de NAT, proviene del NAT dinámico, ya que toma múltiples direcciones IP privadas y las traduce a una única dirección IP pública utilizando diferentes puertos. Se utiliza para sistemas que requieren acceso a de la red pública, pero no tienen que ser visible para el mundo exterior.

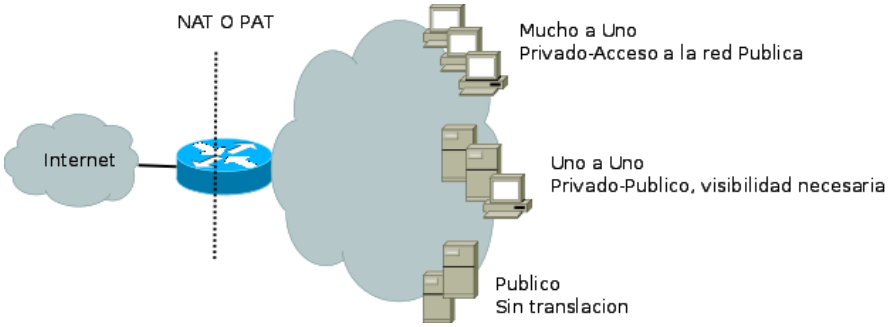


Figura 3-19 Métodos de traducción

Una empresa puede usar ambos direccionamientos, público y privado, según sus necesidades. Por lo tanto, antes de comenzar a diseñar la red es necesario plantearse los siguientes puntos:

- Número de direcciones públicas y privadas que se necesitan
- Número de equipos que requieren acceso a la red publica
- Número de equipos que deben ser visibles al exterior (servidores)
- Donde están los límites entre el direccionamiento público y privado.

Para el IATE solo se requiere direccionamiento privado, aunque todos los hosts necesitan tener acceso a Internet. Inicialmente solo un servidor debe ser visible desde el exterior. El nateo de la dirección publica/privada lo realiza red corporativa, y por tanto el limite entre el direccionamiento público y privado vendrá impuesto por red la corporativa.

Como se dijo con anterioridad, la administración y gestión del router principal y de backup no son objetos de este proyecto. Su responsabilidad recae en Red Corporativa, que es el proveedor de servicios para el IATE, por lo que solo nos proporcionan la IP HSRP de sus routers.

El primer paso en el diseño de un plan de direccionamiento IP es determinar el tamaño de la red para establecer cuántas subredes IP y que número de direcciones IP se necesitan. Para obtener esta información hay que dar respuesta a cuestiones tales como:

- ¿Cuantas sedes componen la red? Requiere recopilar información sobre el número y tipo de localizaciones.
- ¿Cuantas direcciones se necesitan por sede? Implica determinar el número de dispositivos que deben ser direccionado, incluyendo sistemas finales, interfaces router, switches, interfaces firewall, y cualquier otro dispositivo.
- ¿Cuáles son los requisitos de direccionamiento IP para los equipos? Consiste en estudiar si requieren direccionamiento dinámico o estático, público o privado.
- ¿Qué tamaño de subred es adecuada?

La figura que representa la topología general de la red ayuda a determinar el tamaño de la red y su relación con el plan de direccionamiento IP, ya que muestra el número de sedes, su ubicación, y sus relaciones.

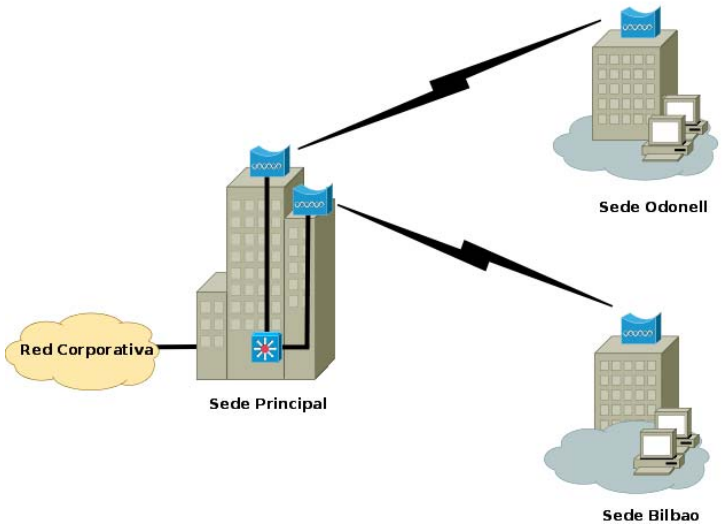


Figura 3-20 Topología de la red de Sevilla (SS.CC.)

El presente proyecto solo abarca la red existente actualmente en Sevilla, sin embargo, un requisito del cliente ha sido tener presente en todo momento que en un plazo máximo de 2 años está planificado el despliegue del IATE por Andalucía. Incluso ha adelantado como dato de partida que el número de trabajadores en cada DD.PP. se estima alrededor de 40. Es por ello que se ha calculado también el direccionamiento previsto para las futuras DD.PP. y los resultados se han incluido en el anexo D de este documento.

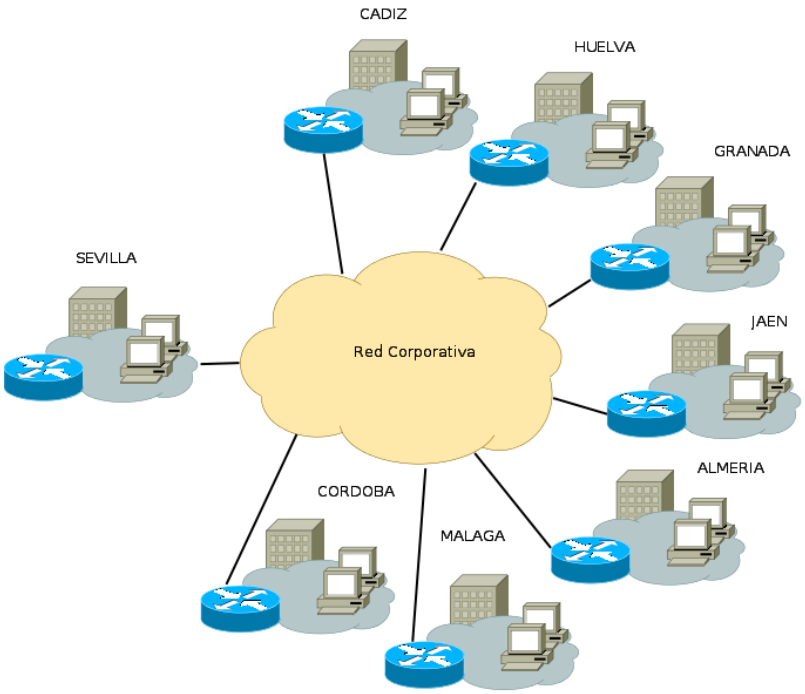


Figura 3-21 Topología de la futura red del IATE

El tamaño de la red, en términos de direccionamiento IP, se relaciona con el número de dispositivos y de interfaces que necesitan una dirección IP. Para permitir el crecimiento de la red sin problemas potenciales es recomendable reservar algunas direcciones adicionales, una práctica habitual suele ser planificar un 30 % de reserva para cada sede.

SEDE	EQUIPOS	RESERVA	TOTAL DE EQUIPOS
SS.CC.	147	30%	192
Cádiz	40	30%	52
Huelva	40	30%	52
Granada	40	30%	52
Jaén	40	30%	52
Almería	40	30%	52
Córdoba	40	30%	52
Málaga	40	30%	52

Tabla 3-6 Requisitos de direcciones IP por sede

La asignación de direcciones incluye asignar una dirección IP a cualquier dispositivo de la red, ya sean equipos, servidores e impresoras. Las dos estrategias básicas de asignación de direcciones IP son:

- **Asignación de IP Estática**: Una dirección IP es asignada manualmente a cada dispositivo. Supone una carga de trabajo adicional ya que el administrador tiene que configurar manualmente todos los parámetros adicionales necesarios, tales como puerta de enlace predeterminada, servidores de nombres, etc...

- **Asignación de IP Dinámica**: Las direcciones IP se asignan dinámicamente a los equipos finales. Supone menos carga para el administrador, pero a cambio, se ve obligado a configurar un servidor para asignar las direcciones, así como definir los grupos de direcciones y parámetros adicionales que deben ser enviados al host. En este caso, el protocolo de configuración dinámica de Servidor (Dynamic Host Configuration Protocol o DHCP) es la solución más fácil, ya que solo requiere que los parámetros sean introducidos en el servidor DHCP, el cual se encarga de enviar la dirección y dichos parámetros al equipo final.

  En términos de seguridad, la asignación dinámica de direcciones IP supone un riesgo mayor que la asignación estática, ya que en la mayoría de los casos, cualquier persona que se conecte a la red puede adquirir una dirección IP válida. Para evitar este problema el DHCP del IATE, tendrá un DHCP con reserva de MAC.

Para decidir entre direccionamiento estático, dinámico o una combinación de ambos, además de sopesar las ventajas e inconvenientes de cada uno, se tienen en consideración los siguientes factores:

- Tipo de nodo: Los dispositivos de red como routers y switches suelen utilizar direccionamiento estático, mientras que los dispositivos de usuario final tales como PCs suelen tener direcciones dinámicas.

- Número de sistemas finales: Si hay más de 30 dispositivos, es preferible usar asignación dinámica. La asignación estática suele utilizarse en redes más pequeñas. En el IATE, el switch de capa 3, Cisco Catalyst serie 3560, es el encargado de asignar las IP dinámicamente a los host.

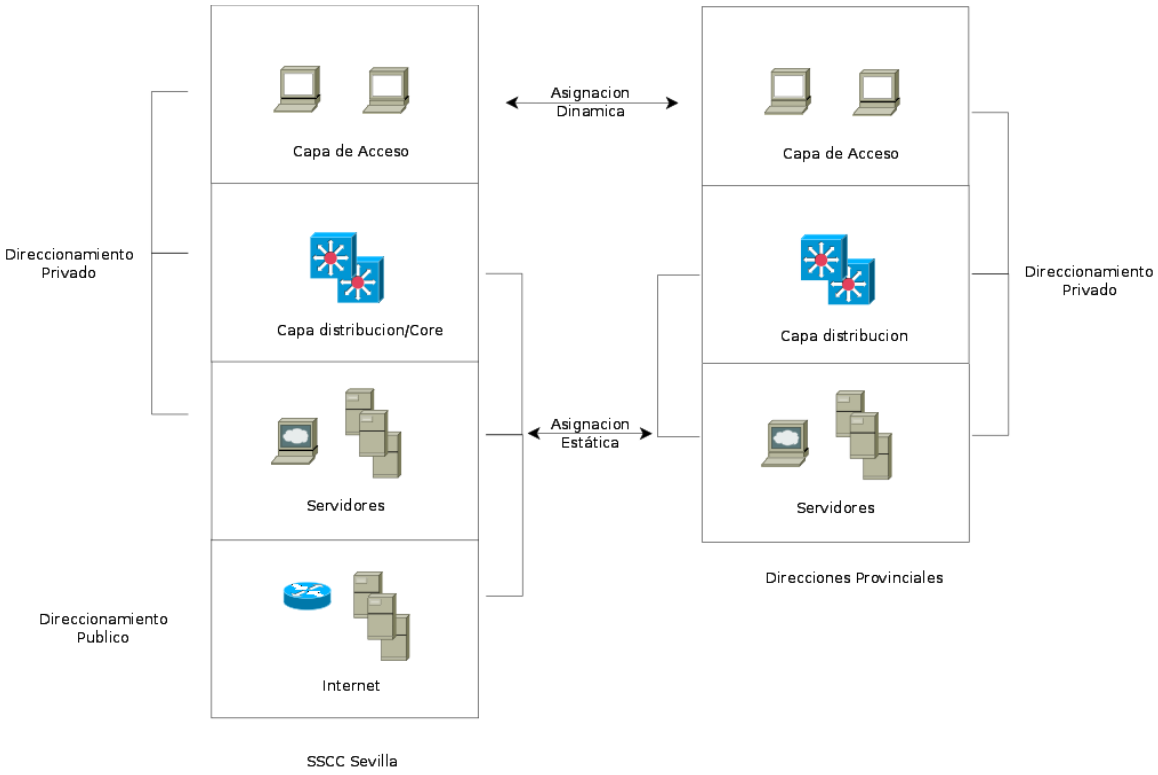


Figura 3-22 Asignación de direcciones IP para el IATE

Llegados a este punto es el momento de usar máscaras de subred de longitud variable (VLSM) para dividir el espacio de direcciones con objeto de alojar las necesidades de direccionamiento de cada edificio.

VLSM representa otra de las tantas soluciones que se implementaron para el agotamiento de direcciones IP y se desarrolló para permitir varios niveles de direcciones IP divididas en subredes dentro de una sola red. Entre sus ventajas ofrece las siguientes:

- Uso más eficiente de las direcciones IP asignadas. Sin el uso de las VLSM, las empresas deben implementar una sola mascara de subred dentro de un numero de red entero de clase A, B o C.

- Reducir la cantidad de información de enrutamiento en el nivel superior, aportando mayor capacidad para utilizar el resumen de ruta, ya que permite más niveles jerárquicos dentro de un plan de direccionamiento.

Como se ha dicho anteriormente, las VLSM permiten dividir en subredes una dirección ya dividida en subredes. Este procedimiento consta de una serie de pasos básicos, los cuales se aplican a continuación para el IATE.

Para calcular las subredes de máscara de subred de longitud variable y los hosts respectivos, primero se asignan los requisitos más grandes del intervalo de direcciones. Los niveles de requisitos se deben enumerar desde el más grande hasta el más pequeño.

- **PASO 1.** Calcular número de subredes necesarias

Dirección dividida en subredes	10.239.64.0/18
Dirección en formato binario	00001010.11101111.01000000.00000000

Tabla 3-7 Cálculo de redes VLSM. Paso 1

El primer paso en el proceso de la división en subredes consiste en dividir la dirección asignada 10.239.64.0/18, en 8 bloques de direcciones del mismo tamaño, puesto que el IATE dispondrá de 8 DD.PP, y dado que $2^3 = 8$, el número total de bits necesarios para identificar a cada una de las 8 subredes es 3.

DIRECCIÓN ASIGNADA	SUBREDES	DESCRIPCIÓN
10.239.64.0/18	10.239.64.0/21	**Sede #1 del IATE**
	10.239.72.0/21	**Futura Sede #2 del IATE**
	10.239.80.0/21	**Futura Sede #3 del IATE**
	10.239.88.0/21	**Futura Sede #4 del IATE**
	10.239.96.0/21	**Futura Sede #5 del IATE**
	10.239.104.0/21	**Futura Sede #6 del IATE**
	10.239.112.0/21	**Futura Sede #7 del IATE**
	10.239.120.0/21	**Futura Sede #8 del IATE**

Tabla 3-8 Cálculo de redes VLSM para el IATE. Paso 1

- **PASO 2.** Calcular redes VLSM para SS.CC.

En SS.CC. se necesitan las siguientes divisiones: DMZ, Informática, Olivé, Servidores, Bilbao, O'Donnell, Wireless y Administración. En total 8, por lo que se requieren 3 bits de los 8 del tercer octeto para la máscara VLSM que identificará cada departamento.

La primera dirección disponible es 10.239.64.0/21. Según la Tabla 3-6, SS.CC. es la sede que requiere más hosts, concretamente 192, por lo que hay que usar 8 bits, dado que $2^8 - 2$

= 254 direcciones de hosts utilizables. De manera que se utilizarán los 8 bits del cuarto octeto para las direcciones de hosts. Al tratarse de direccionamiento privado no supone ningún problema reservar un numero elevado de IPs por subred. La representación binaria de bits disponibles quedaría como sigue:

		TERCER OCTETO								CUARTO OCTETO							
10.	239.	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RED	SUBRED			Sede #1			Dpto ##			HOST ##							
				SUBRED VLSM													

Tabla 3-9 Representación binaria de bits disponibles para la sede de SS.CC.

El resultado de la división en subredes para SS.CC. se muestra en la siguiente tabla.

DIRECCIÓN ASIGNADA A SEDE #1	SUBREDES DENTRO DE SEDE #1					DESCRIPCIÓN
		RED / SUBRED		Sede #1 SS.CC.	Dpto ##	HOST	
10.239.64.0/21	10.239.64.0/24	10. 239.	01	000	000	00000000	DMZ
	10.239.65.0/24				001		Informática
	10.239.66.0/24				010		Olivé
	10.239.67.0/24				011		Servidores
	10.239.68.0/24				100		Bilbao
	10.239.69.0/24				101		O'Donnell
	10.239.70.0/24				110		Wireless
	10.239.71.0/24				111		Administración

Tabla 3-10 Cálculo de redes VLSM para SS.CC. Paso 2

- **PASO 3.** Calcular redes VLSM para las futuras DD.PP.

El siguiente paso consiste en realizar un procedimiento similar para cada una de las futuras DD.PP. Como se ha comentado anteriormente, el resultado obtenido se ha incluido en el Anexo D del presente documento, Direccionamiento de las futuras DD.PP.

3.8 VLANs

Una VLAN, acrónimo de Virtual LAN o red de área local virtual, es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del Dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un switch capa 3 y 4).

Una VLAN consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo conmutador, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles.

3.8.1 Ventajas de la creación de VLANs

La productividad del usuario y la adaptabilidad de la red son impulsores claves para el crecimiento y el éxito de la empresa. La implementación de la tecnología de VLANs permite que una red admita de manera más flexible las metas comerciales. Sus principales beneficios son los siguientes:

- Seguridad. Los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial.
- Reducción de costos al no necesitar actualizaciones caras del equipamiento de red, así como a un uso más eficiente de los enlaces y del ancho de banda existente.
- Mayor rendimiento. La división de las redes planas de Capa 2 en múltiples grupos lógicos de trabajo (dominios de broadcast) reduce el tráfico innecesario en la red y potencia el rendimiento.
- Mitigación de la tormenta de broadcast, ya que reduce el número de dispositivos que pueden participar en una tormenta de broadcast e impide que se propague a toda la red.
- Mayor eficiencia del personal de Tecnologías de la información. Las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN.

3.8.2 Asignación de VLANs

Para la asignación de VLANs en el diseño de la nueva red jerárquica es recomendable seguir, en la medida de lo posible, las siguientes pautas:

1. Asociar una VLAN a cada subred.
2. Configurar el enrutamiento entre VLANs usando switches de capa 3.
3. Asociar los usuarios finales de una VLAN a un stack específico de switches. Lo ideal es limitar las VLAN a un switch de acceso o un stack de switch, sin embargo, puede ser necesario extender una VLAN a través de múltiple switch dentro de un stack de switches para soportar otras prestaciones, tales como la movilidad inalámbrica.

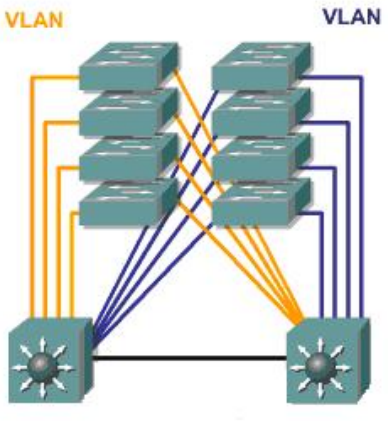


Figura 3-23 Asignación de VLANs

El resultado de aplicar estos pasos a SS.CC. se muestra en la siguiente tabla, mientras que la asignación de VLANs en las futuras DD.PP. se recoge en el Anexo D.

DIRECCIÓN ASIGNADA A SEDE #1	SUBREDES DENTRO DE SEDE #1	DESCRIPCIÓN	VLAN ## DE SS.CC
10.239.64.0/21	10.239.64.0/24	DMZ	**VLAN #1**
	10.239.65.0/24	Informática	**VLAN #2**
	10.239.66.0/24	Olivé	**VLAN #3**
	10.239.67.0/24	Servidores	**VLAN #4**
	10.239.68.0/24	Bilbao	**VLAN #5**
	10.239.69.0/24	O'Donnell	**VLAN #6**
	10.239.70.0/24	Wireless	**VLAN #7**
	10.239.71.0/24	Administración	**VLAN #8**

Tabla 3-11 Asignación de VLANs a la red del IATE

3.9 Enrutamiento entre VLANs

Los switches soportan múltiples VLANs pero no tienen capacidad para enrutar paquetes entre ellas, por lo que deben conectarse a un dispositivo de capa 3 que permita dicho enrutamiento. Para solventar esta situación existen varias alternativas, presentadas a continuación:

- **Usar un router.** Esta opción tiene como ventajas que su implementación es sencilla, no son necesarios los servicios de nivel 3 en el switch y además el router proporciona comunicaciones entre VLANs. En su contra, el router es un punto único de fallo, la ruta del tráfico de ida entre el switch y el router puede ser congestionado y la latencia es más alta que la de un switch de capa 3.

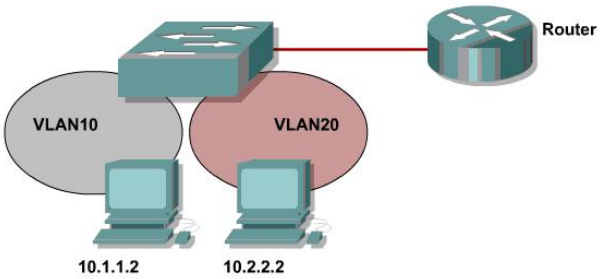


Figura 3-24 Enrutamiento entre VLANs usando router

La conectividad entre VLANs se puede lograr a través de una conectividad lógica o física. La conectividad lógica involucra una conexión única, o un enlace troncal, desde el switch hasta el router. Ese enlace troncal puede admitir varias VLANs. Esta topología se conoce como “router en un palo” porque, como se aprecia en la figura, existe una sola conexión al router. Sin embargo, existen varias conexiones lógicas entre el router y el switch. La conectividad física implica una conexión física separada para cada VLAN. Esto significa una interfaz física separada para cada VLAN.

En este enfoque, el tráfico entre VLANs debe atravesar el backbone de Capa 2 para alcanzar el router desde donde podrá desplazarse entre las VLAN. El tráfico viaja entonces de vuelta hacia la estación final deseada utilizando el método de envío de Capa 2 normal. Este flujo de ida y vuelta es característico del diseño "router en un palo".

- **Switch multicapas, o switch de capa 3.** Tradicionalmente los switches toman decisiones de envío analizando la cabecera de la capa 2, mientras que un router lo hace analizando la cabecera de la capa 3. Un switch múlticapa combina la funcionalidad de un switch y un router en un solo dispositivo, por lo tanto, permite que el dispositivo pueda reenviar el tráfico cuando el origen y destino están en la misma VLAN, y enrutarlo cuando el origen y destino están en distintas redes.

La principal diferencia entre la operación de conmutación de paquetes de un router y la de un switch de capa 3 es la implementación física. En general, en los routers, la conmutación de paquetes se realiza mediante un microprocesador, mientras que un switch de capa 3, esta operación se realiza usando hardware, application-specific-integrated-circuit (ASIC). Esto hace que los switch tengan rendimientos de conmutación de paquetes medidos en millones de paquetes por segundo (pps), mientras que en general los routers tradicionales han evolucionado desde los 100.000 pps hasta un millón de pps.

Por los motivos expuestos anteriormente, tales como menor latencia, mayor velocidad de reenvío y alta disponibilidad, para el IATE la opción elegida ha sido el switch de capa 3.

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.239.128.4 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 8 subnets
C       10.239.128.0 is directly connected, GigabitEthernet0/23
C       10.239.69.0 is directly connected, Vlan6
C       10.239.68.0 is directly connected, Vlan5
C       10.239.71.0 is directly connected, Vlan8
C       10.239.70.0 is directly connected, Vlan7
C       10.239.65.0 is directly connected, Vlan2
C       10.239.67.0 is directly connected, Vlan4
C       10.239.66.0 is directly connected, Vlan3
S*   0.0.0.0/0 [1/0] via 10.239.128.4
```

Figura 3-25 Tabla de enrutamiento entre VLANs para SS.CC.

Como se observa en la Figura 3-25, existe una entrada en la tabla de rutas por cada subred del IATE. Cada subred a su vez se asocia a una VLAN. Cada VLAN es una interfaz virtual del switch de capa 3 (Switch Virtual Interface o SVI). Además las SVI se puede ver que están conectadas, así que cualquier paquete que entre con destino hacia alguna de las VLAN, será enrutado por el switch a la VLAN indicada. Por ultimo se puede apreciar que la dirección de Gateway es la 10.239.128.4, que se corresponde con la pata del firewall del IATE, el cual está conectado al switch por la interfaz GigabitEthernet 0/23.

Como medida de seguridad se utilizarán VACL (VLAN Access Control Lists), para impedir el paso de determinados paquetes de una VLAN a otra, y RACL (Router based Access List). Esto se tratará con mayor detalle posteriormente en el capitulo de seguridad.

A continuación se incluyen las listas de verificación para VLANs del IATE, direccionamiento estático y dinámico.

Lista de verificación VLANs		
Requerimiento:	➢ **REQ_01**: El administrador de red debe asegurar tanto el alta de las VLAN en el switch, como de sus interfaces virtuales.	
Procedimiento:	Definición de las VLAN y posteriormente asignación de las IPs, en caso de ser necesario.	
Pasos	**Instrucciones**	**Estado**
1	Alta de las VLANs.	Realizado
2	Configuración interfaces virtuales. Crear una interfaz virtual por cada VLAN en los switches ScSwitch01 y ScSwitch02. Ver Tabla 3-13 IPs SVI / VLANs.	Realizado
3	Propagación / Configuración de las VLANs a los switch de acceso. Los switches de acceso al utilizar enlaces troncales deben recibir automáticamente las configuraciones de las VLANs. Sin embargo, en el caso de Bilbao y O'Donell, como los puentes inalámbricos no soportan enlaces troncales, la configuración debe ser manual.	Realizado

Tabla 3-12 Lista de verificación VLANs

ScSwith01, Catalyst 3560		
Interfaz	**IP / Mascara de Subred**	**IP Dinámica/Estática**
VLAN 2	10.239.65.2	Estático
VLAN 3	10.239.66.2	Estático
VLAN 4	10.239.67.2	Estático
VLAN 5	10.239.68.2	Estático
VLAN 6	10.239.69.2	Estático
VLAN 7	10.239.70.2	Estático
VLAN 8	10.239.71.2	Estático

ScSwith02, Catalyst 3560		
Interfaz	**IP / Mascara de Subred**	**IP Dinámica/Estática**
VLAN 2	10.239.65.3	Estático
VLAN 3	10.239.66.3	Estático
VLAN 4	10.239.67.3	Estático
VLAN 5	10.239.68.3	Estático
VLAN 6	10.239.69.3	Estático
VLAN 7	10.239.70.3	Estático
VLAN 8	10.239.71.3	Estático

Tabla 3-13 IPs SVI / VLANs

Lista de verificación Direccionamiento Estático		
Requerimiento:	➢ **REQ_02:** El administrador debe proporcionar el direccionamiento correcto a los dispositivos que requieren una dirección estática	
Procedimiento:	El administrador mantiene un documento con las IP asignadas y libres.	
Pasos	**Instrucciones**	**Estado**
1	Asignación estática a las IPs de las interfaces de administración de los switches. Ver Tabla 3-15 IPs de las interfaces de administración	Realizado
2	Asignación estática a las IPs de las interfaces de los switches principal y de backup. Ver Tabla 3-16 IPs SVI para ScSwitch01 y Tabla 3-17 IPs SVI para ScSwitch02	Realizado
3	Asignación de IPs estáticas a los servidores, tanto de la DMZ como de la VLAN de servidores. Ver Tabla 3-18 IPs estáticas **para servidores**	Realizado
4	Asignación de IPs estáticas a las impresoras. Ver Tabla 3-19 IPs estáticas para impresoras	Realizado
5	Asignación de IPs estáticas a las SAIs. Ver Tabla 3-20 IPs estáticas para SAIs	Realizado

Tabla 3-14 Lista de verificación Direccionamiento Estático

Switch	Interfaz	IP / Mascara de Subred	Información de la localización
ScSwitch03	VLAN 8	10.239.71.103	CPD
ScSwitch04	VLAN 8	10.239.71.104	CPD
ScSwitch05	VLAN 8	10.239.71.105	CPD
ScSwitch06	VLAN 8	10.239.71.106	CPD
ScSwitch07	VLAN 8	10.239.71.107	CPD
ScSwitch11	VLAN 8	10.239.71.111	Muñoz Olivé
ScSwitch12	VLAN 8	10.239.71.112	Muñoz Olivé
ScSwitch13	VLAN 8	10.239.71.113	Muñoz Olivé
ScSwitch14	VLAN 8	10.239.71.114	Muñoz Olivé
ScExterno	VLAN 8	10.239.71.115	Muñoz Olivé
BiSwitch01	VLAN 5	10.239.68.241	Bilbao
BiSwitch02	VLAN 5	10.239.68.242	Bilbao
BiSwitch03	VLAN 5	10.239.68.243	Bilbao
OdSwitch01	VLAN 6	10.239.69.241	O'Donell
OdSwitch02	VLAN 6	10.239.69.242	O'Donell
PuenteSsccBilbao	VLAN 5	10.239.68.253	CPD
PuenteSssccOdonell	VLAN 6	10.239.69.253	CPD
PuenteBilbao	VLAN 5	10.239.68.254	Bilbao
PuenteOdonell	VLAN 6	10.239.69.254	O'Donell

Tabla 3-15 IPs de las interfaces de administración

ScSwitch01			
Interfaz SVI	**IP / Mascara de Subred**	**Protocolo de Enrutamiento**	**Información de la localización**
VLAN 2	10.239.65.2	Estático	CPD
VLAN 3	10.239.66.2	Estático	CPD
VLAN 4	10.239.67.2	Estático	CPD
VLAN 5	10.239.68.2	Estático	CPD
VLAN 6	10.239.69.2	Estático	CPD
VLAN 7	10.239.70.2	Estático	CPD
VLAN 8	10.239.71.2	Estático	CPD
Gi0/23	10.239.128.2	Estático	CPD

Tabla 3-16 IPs SVI para ScSwitch01

ScSwitch02			
Interfaz SVI	**IP / Mascara de Subred**	**Protocolo de Enrutamiento**	**Información de la localización**
VLAN 2	10.239.65.3	Estático	CPD
VLAN 3	10.239.66.3	Estático	CPD
VLAN 4	10.239.67.3	Estático	CPD
VLAN 5	10.239.68.3	Estático	CPD
VLAN 6	10.239.69.3	Estático	CPD
VLAN 7	10.239.70.3	Estático	CPD
VLAN 8	10.239.71.3	Estático	CPD
Gi0/23	10.239.128.3	Estático	CPD

Tabla 3-17 IPs SVI para ScSwitch02

Nombre del dispositivo	Función	Sistema Operativo	IP/Mascara	VLAN
Hades	Webserver	Linux	10.239.64.16	DMZ
Cervero1	Firewall1	Linux	10.239.64.2	DMZ
Cervero2	Firewall2	Linux	10.239.64.3	DMZ
Neptuno	DBServer1	Linux	10.239.67.100	VLAN 4
Hefesto	Webinterno	Linux	10.239.67.101	VLAN 4
Desarrollo1	Desarrollo	Linux	10.239.67.102	VLAN 4
Desarrollo2	Desarrollo	Linux	10.239.67.103	VLAN 4
Poseidon	DBServer2	Linux	10.239.67.104	VLAN 4
Atenea1	Proxy	Linux	10.239.67.105	VLAN 4
Atenea2	DNS	Linux	10.239.67.106	VLAN 4
Afrodita	Dominio1	Linux	10.239.67.107	VLAN 4
Helios	Monitorización	Linux	10.239.67.108	VLAN 4
Apolo	Servidor de Impresión	Windows 2003	10.239.67.109	VLAN 4
Backup	Backup	Windows 2003	10.239.67.110	VLAN 4

Tabla 3-18 IPs estáticas para servidores

Nombre del dispositivo	IP/Mascara	VLAN
Konica Minolta	10.239.65.200	VLAN 2
Konica Minolta	10.239.65.201	VLAN 2
Konica Minolta	10.239.66.200	VLAN 3
Konica Minolta	10.239.66.201	VLAN 3
Konica Minolta	10.239.66.202	VLAN 3
Konica Minolta	10.239.66.203	VLAN 3
Konica Minolta	10.239.66.204	VLAN 3
Konica Minolta	10.239.66.205	VLAN 3
Konica Minolta	10.239.66.206	VLAN 3
Gestener	10.239.66.207	VLAN 3
Gestener	10.239.66.208	VLAN 3
Konica Minolta	10.239.68.200	VLAN 5
Konica Minolta	10.239.68.202	VLAN 5
Konica Minolta	10.239.68.203	VLAN 5
Konica Minolta	10.239.68.204	VLAN 5
Konica Minolta	10.239.68.205	VLAN 5
Konica Minolta	10.239.68.206	VLAN 5
Gestener	10.239.68.207	VLAN 5

Gestener	10.239.68.208	VLAN 5
Gestener	10.239.68.208	VLAN 5
Gestener	10.239.68.208	VLAN 5
Konica Minolta	10.239.69.200	VLAN 5
Konica Minolta	10.239.69.201	VLAN 5
Konica Minolta	10.239.69.202	VLAN 5
Gestener	10.239.69.203	VLAN 5
Gestener	10.239.69.204	VLAN 5

Tabla 3-19 IPs estáticas para impresoras

SAI	IP/Mascara	Vlan
Sai01	10.239.67.251	VLAN 4
Sai02	10.239.67.252	VLAN 4
Sai03	10.239.67.253	VLAN 4
Sai04	10.239.66.254	VLAN 3
BiSai01	10.239.68.251	VLAN 5
OdSai01	10.239.69.251	VLAN 6

Tabla 3-20 IPs estáticas para SAIs

Lista de verificación Direccionamiento Dinámico		
Requerimiento:	➢ **REQ_03:** El administrador debe proporcionar IP a los equipos que han solicitado el alta en el DHCP.	
Procedimiento:	El administrador concede IP para aquellos equipos que tenga su MAC registrada en el DHCP.	
Pasos	**Instrucciones**	**Estado**
1	Asignación de IP dinámica a los usuarios de Informática con reserva de MAC. Todos los usuarios que requieran uso de la red deberán hacer una petición, solicitando el alta en el DHCP.	Realizado
2	Asignación de IP dinámica a los usuarios de Muñoz Olivé con reserva de MAC. Todos los usuarios que requieran uso de la red deberán hacer una petición, solicitando el alta en el DHCP.	Realizado
3	Asignación de IP dinámica a los usuarios de Bilbao con reserva de MAC. Todos los usuarios que requieran uso de la red deberán hacer una petición, solicitando el alta en el DHCP.	Realizado
4	Asignación de IP dinámica a los usuarios de O'Donell con reserva de MAC. Todos los usuarios que requieran uso de la red deberán hacer una petición, solicitando el alta en el DHCP.	Realizado

Tabla 3-21 Lista de verificación Direccionamiento Dinámico

3.10 Redundancia

3.10.1 Redundancia Capa 2 – Protocolo STP

Las empresas modernas dependen cada vez más de su red. La inactividad de la red se traduce en pérdida de negocios e ingresos, y desconfianza en los clientes.

Si existe un único punto de fallo en la red, su caída hace que el tiempo de inactividad de la red produzca tiempo de inactividad en la empresa. La redundancia es necesaria en el diseño de la red con el fin de mantener un alto grado de fiabilidad y eliminar cualquier punto único de fallo, y se logra mediante la instalación en las áreas críticas de tanto equipos duplicados como enlaces de red. Con la redundancia se consigue tener dos vías alternativas para un destino en particular.

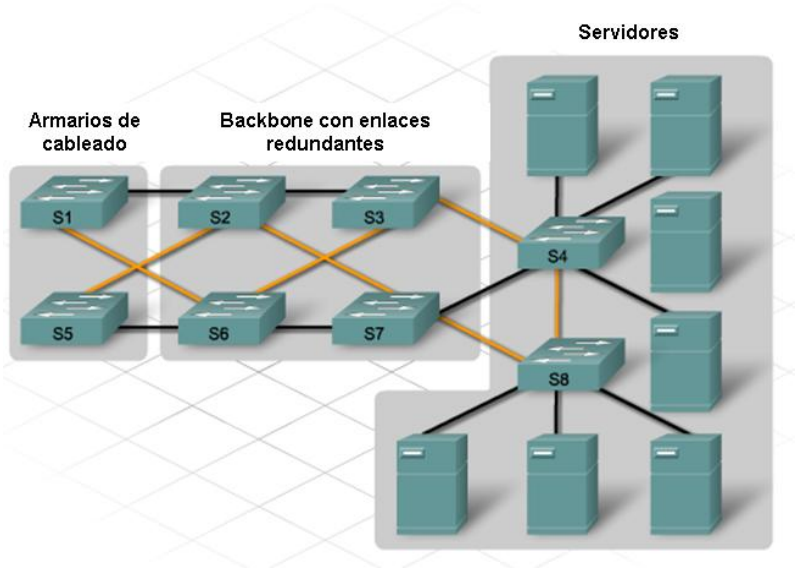


Figura 3-26 Redundancia en capa 2

Ejemplos de redundancia en la vida real son dos carreteras en una ciudad o dos puertas para salir de un edificio, si se bloquea una, la otra estaría todavía disponible. Para lograr la redundancia en la electrónica de red, se utilizan conexiones con múltiples enlaces. Los enlaces redundantes en una red conmutada ayudan a reducir la congestión y dan soporte a la alta disponibilidad y al balanceo de carga.

La siguiente figura muestra dos ejemplos de redundancia en una red jerárquica. En el primero de ellos, el PC1 se comunica con el PC4 a través del enlace troncal1. En el segundo caso, el switch S2 detecta la conexión interrumpida al switch S1 y cambia su ruta de envío para pasar a través del switch S3.

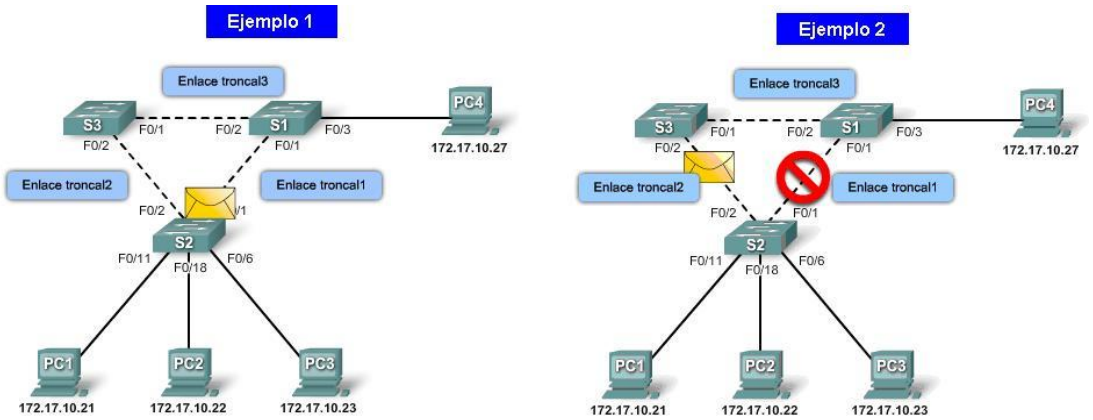


Figura 3-27 Redundancia en una red jerárquica

Sin embargo, la redundancia también tiene sus inconvenientes, si no está bien configurada, puede causar problemas. Por ejemplo, la naturaleza de difusión del tráfico Ethernet crea bucles. Las tramas de difusión, cuando se produce un bucle, causan una tormenta de difusión, que deriva en una utilización de todo el ancho de banda disponible, cuya consecuencia puede ser pérdida de las conexiones establecidas y caída de toda la red. Para tratar de resolver el problema de los bucles y las tormentas de difusión en redes conmutadas surgió el protocolo Spanning Tree (STP).

Cuando un protocolo de propiedad es tan predominante que todos sus competidores del mercado deben contar con soporte para el mismo, las agencias como el IEEE intervienen y crean una especificación pública. La evolución de STP ha seguido este mismo camino, como puede verse en la siguiente tabla, de ahí que existan muchos tipos de variantes de STP, algunas de ellas propiedad de Cisco y otras estándares de IEEE.

PROPIEDAD DE CISCO	
STP por VLAN (PVST)	▪ Utiliza el protocolo de enlace troncal Inter Switch Link (ISL) propiedad de Cisco, que permite que un enlace troncal se encuentre en estado de enviar para algunas VLAN y en estado de bloqueo para otras. ▪ Cada VLAN cuenta con una instancia de Spanning Tree ▪ Capacidad para balancear la carga de tráfico de la capa 2 ▪ Incluye las extensiones propiedad de Cisco BackboneFast, UplinkFast y PortFast
PVST+	▪ Admite ISL y enlace troncal IEEE 802.1Q ▪ Proporciona la misma funcionalidad que PVST, incluidas las extensiones de STP propiedad de Cisco. No cuenta con soporte en dispositivos que no son de Cisco.

	▪ Agrega mejoras PortFast denominadas protección de BPDU (Bridge Protocol Data Units) y protección de raíz
PVST+ rápido	▪ Basado en el estándar IEEE 802.1w ▪ Posee convergencia más veloz que STP (estándar 802.1D) ▪ Incluye las extensiones propiedad de Cisco BackboneFast, UplinkFast y PortFast
ESTÁNDAR IEEE	
Rapid STP (RSTP)	▪ Presentado en 1982, brinda convergencia más veloz que STP (estándar 802.1D) ▪ Implementa versiones genéricas de las extensiones de STP propiedad de Cisco como BackboneFast, UplinkFast y PortFast en el estándar público. ▪ IEEE incorporó RSTP dentro de 802.1D, identificando la especificación como IEEE 802.1D-2004
Múltiple STP (MSTP)	▪ Pueden asignarse varias VLAN a una misma instancia de Spanning Tree, de tal modo que se reduce la cantidad de instancias necesarias para admitir un gran número de VLANs. ▪ Inspirado en el protocolo de Spanning Tree de múltiples instancias (MISTP) de Cisco. Es una evolución de STP y RSTP. ▪ Proporciona varias rutas de envío para el tráfico de datos y permite el balanceo de carga. ▪ IEEE 802.1Q-2003 ahora incluye a MSTP

Tabla 3-22 Variantes de Cisco y STP

STP es un protocolo abierto, transparente a las estaciones de trabajo. Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología está libre de bucles y que por tanto existe una sola ruta lógica entre todos los destinos de la red.

Un puerto se considera bloqueado cuando el tráfico de la red no puede ingresar ni salir de él. El bloqueo de las rutas redundantes es fundamental para evitar bucles en la red. Las rutas físicas aún existen para proporcionar la redundancia, pero las mismas se deshabilitan para evitar que se generen bucles. Si alguna vez las rutas bloqueadas son necesarias para compensar un fallo en un

cable de la red o un switch, STP vuelve a calcular las rutas y desbloquea los puertos necesarios para permitir que la ruta redundante se active.

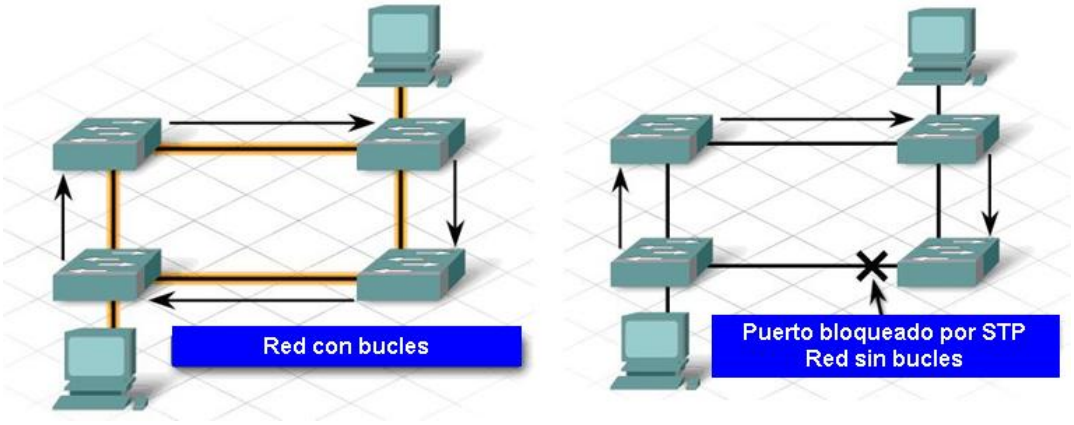


Figura 3-28 Eliminación de bucles por el Protocolo STP

STP es relativamente autosuficiente y requiere de muy poca configuración. Utiliza el algoritmo de Spanning Tree (STA) para determinar que puertos del switch deben configurarse en estado bloqueado. Este algoritmo cambia una red física con forma de malla, en la que existen bucles, por una red lógica en árbol en la que no existe ningún bucle. El STA designa un único switch como puente raíz y lo utiliza como punto de referencia para todos los cálculos de rutas. Los puentes se comunican mediante mensajes de configuración llamados Bridge Protocol Data Units (BPDU).

El protocolo establece identificadores de puente y elige el que tiene la prioridad más baja como puente raíz. Por tanto, la primera decisión que toman todos los switches de la red es identificar dicho puente raíz, ya que esto afectará al flujo de tráfico. Para ello intercambian tramas BPDU con el fin de determinar el switch que posee el menor ID de puente (BID) en la red, que será el que se transforme de forma automática en el puente raíz.

Después de determinar el puente raíz, el STA calcula la ruta más corta hacia el mismo. Seguidamente, entre todos los puentes que conectan un segmento de red, se elige un puente designado, el de menor coste para transmitir las tramas hacia la raíz. En el caso de que haya mismo coste en dos puentes, se elige el puente con menor BID.

Para cada puente se calcula cual de sus puertos tiene menor coste al puente raíz, ese será el puerto raíz de ese puente. En caso de empate, el switch debe determinar cuál de los dos puertos es el puerto raíz.

Una vez elegido el puente raíz y los puertos raíz de los otros puentes se pasa a calcular los puertos designados de cada LAN, que será el que ofrece un camino de menor coste hacia el

puente raíz. Si hubiese empate se elige por el ID más bajo. Aquellos puertos que no sean elegidos como raíz ni como designados deben bloquearse.

Cuando el STA determina las rutas que deben permanecer disponibles, configura los puertos de switch de acuerdo a distintas funciones. Las funciones de los puertos describen su relación en la red con el puente raíz y si los mismos pueden enviar tráfico.

Puertos deshabilitados	Es un puerto de switch que está administrativamente desconectado. Un puerto deshabilitado no funciona en el proceso de spanning-tree.
Puertos no designados	Son todos los puertos configurados en estado de bloqueo para poder romper de forma lógica la topología de bucle. Cuando un puerto se encuentra en estado bloqueado, no puede reenviar tráfico.
Puertos designados	Existen en los puentes raíz y en los que no son raíz. Los puertos designados se encuentran normalmente en estado de reenvío, transmitiendo el tráfico por el segmento. ▪ Para los puentes raíz, todos los puertos de switch son designados. ▪ Para los puentes que no son raíz, un puerto designado es el switch que recibe y envía tramas hacia el puente raíz según sea necesario. Sólo se permite un puerto designado por segmento. Como se ha dicho en párrafos anteriores, si existen varios switches en el mismo segmento, un proceso de elección determina el switch designado
Puertos raíz	Existe en los puentes que no son raíz y es el puerto de switch con la mejor ruta hacia el puente raíz. Estos puertos se encuentran normalmente en estado de reenvío. Sólo se permite un puerto raíz por puente. Para cada puente se calcula cual de sus puertos tiene menor coste al puente raíz, ese será el puerto raíz de ese puente. En caso de empate, el switch debe determinar cuál de los puertos es el puerto raíz, para ello utiliza el valor de prioridad de puerto personalizable. Los valores de prioridad de puerto oscilan entre 0 y 240, en incrementos de 16, y el valor predeterminado es 128. Los valores de prioridad de puerto menores proporcionan al puerto una mayor prioridad o el menor ID de puerto si ambos valores de prioridad de puerto coinciden. El ID de puerto es el identificador de interfaz del puerto y está adjunto a la prioridad de dicho puerto.

Tabla 3-23 Protocolo STP. Funciones de los puertos

Por tanto, los pasos que sigue STP para converger en una topología de red libre de bucles básicamente se pueden resumir en los siguientes puntos:

1. Elección de un puente raíz.
2. Selección del puerto raíz en los puentes no raíz.
3. Selección del puerto designado en cada segmento.

En el siguiente ejemplo, el puente raíz es el switch S1, escogido a través de un proceso de elección, y el STA configura los puertos del siguiente modo:

Switch S1

- ✓ Puerto F0/1 → Configurado como puerto designado.
- ✓ Puerto F0/2 → Configurado como puerto designado.

Switch S2

- ✓ Puerto F0/1 → Configurado como puerto raíz para el enlace troncal entre el switch S2 y el switch S1.
- ✓ Puerto F0/2 → Configurado como puerto designado.

Switch S3

- ✓ Puerto F0/1 → Configurado como puerto raíz para el enlace troncal entre el switch S3 y el switch S1.
- ✓ Puerto F0/2 → Función no designado, ya que se encuentra en estado de bloqueo.

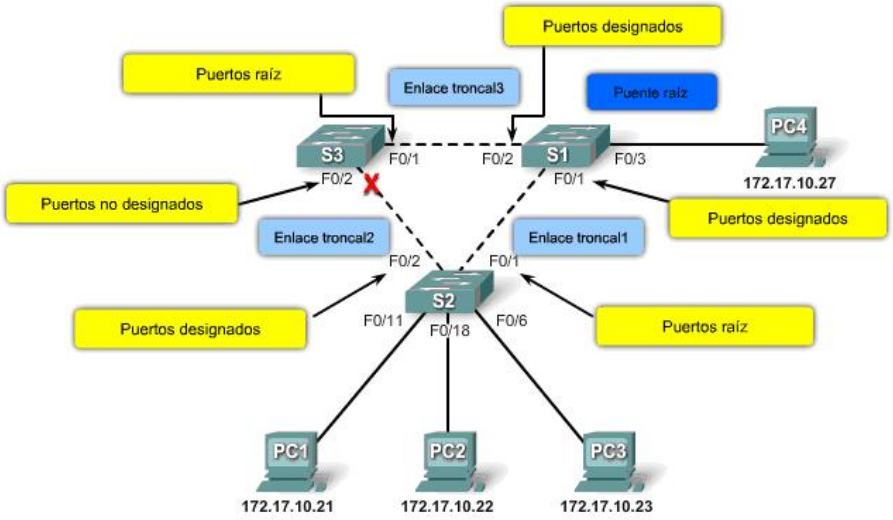


Figura 3-29 Protocolo STP – Ejemplo de funciones de los puertos

Las BPDUs de configuración son tramas multicast enviadas por defecto cada 2 segundos a todos los switches. La trama de BPDU contiene 12 campos distintos que proporcionan información de prioridad y de ruta, requerida por el protocolo STP para la elección del puente raíz y el cálculo de las rutas al mismo.

- **Protocol Identifier**. Tipo de protocolo utilizado. Siempre es 0.
- **Version**. Versión del protocolo. Siempre es 0.
- **Message Type**. Tipo de BPDU (De configuración o de notificación de cambio en la topología)
- **Flags**. Usados para manejar cambios en la topología activa.
- **Root ID**. Contiene el BID del Puente Raíz.
- **Root Path Cost**. Coste acumulativo hasta el Puente Raiz.
- **Bridge ID**. Identificador del Puente que envía la BPDU.
- **Port ID**. Identificador del Puerto que envía la BDPU.
- **Message Age**. Cantidad de tiempo desde que el puente raíz envío el mensaje de configuración sobre el cual se basa la actual BPDU.
- **Max Age**. Muestra el tiempo máximo que la BPDU debe ser almacenada.
- **Hello Time**. Periodo de tiempo entre mensajes de configuración del puente raíz.
- **Forward Delay.** Tiempo que deben esperar los switches antes de cambiar a un nuevo estado después un cambio de topología.

Figura 3-30 Protocolo STP – Estructura BPDU

Como se ha visto anteriormente, el identificador de puente en la red se utiliza durante la elección del puente raíz. En la Figura 3-31 se observa que el BID contiene un valor de prioridad, la dirección MAC del switch emisor y opcionalmente un ID de sistema extendido. El BID de menor valor se determina mediante la combinación de estos tres campos.

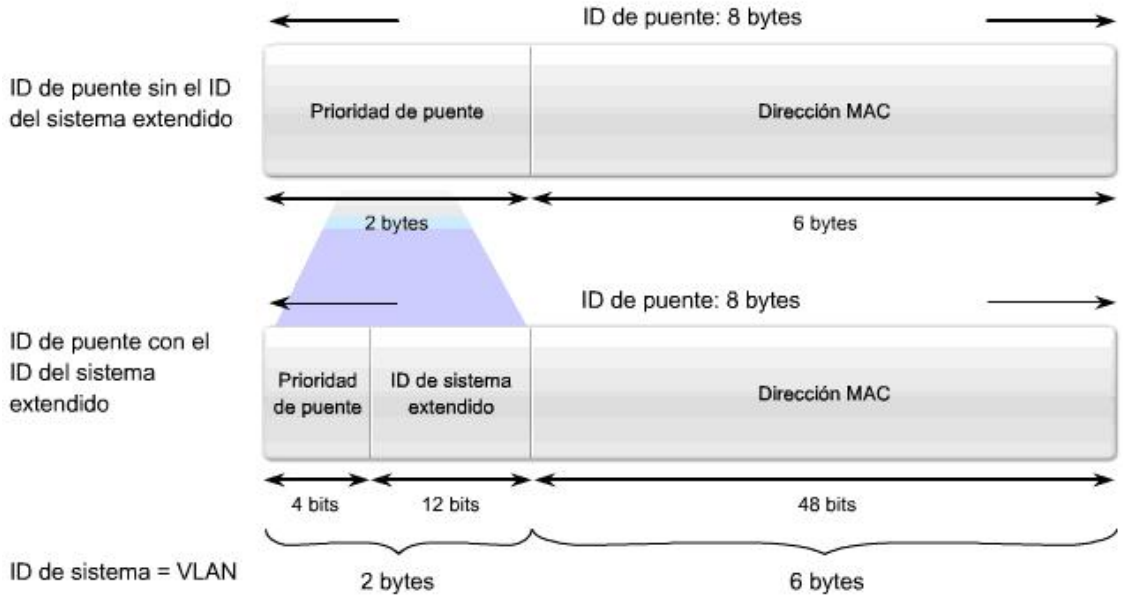


Figura 3-31 Protocolo STP – Campos BID

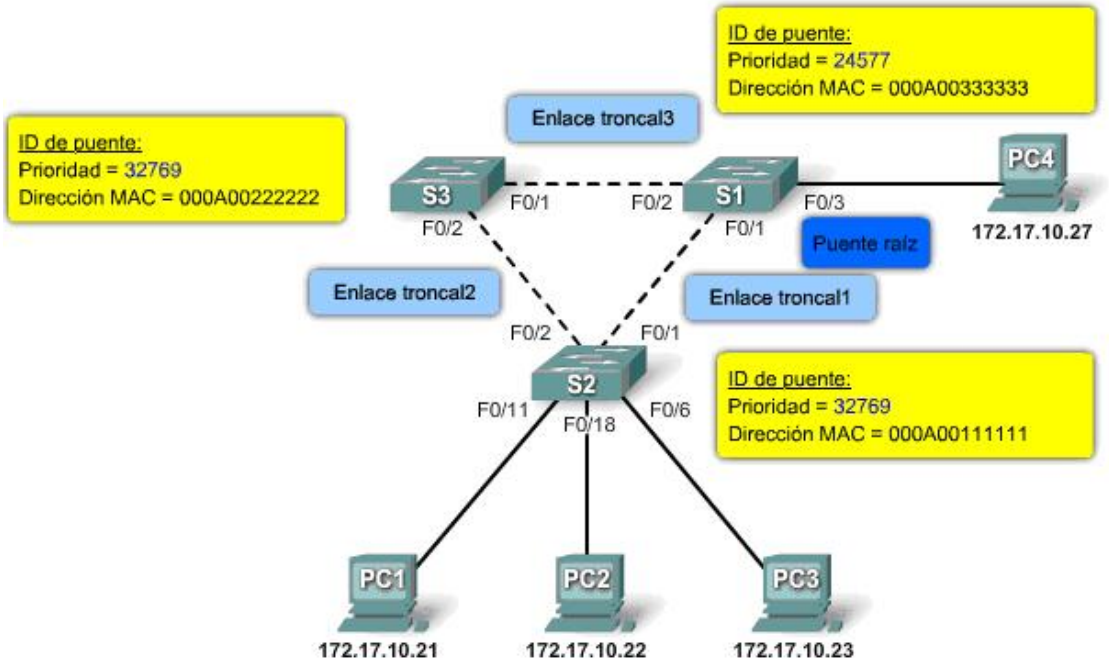


Figura 3-32 Protocolo STP – Ejemplo selección de Puente raíz

El Coste de la Ruta raíz (Root Path Cost) es también un valor significativo para las elecciones STP, ya que el STA comienza el proceso determinando las mejores rutas hacia el puente raíz desde todos los destinos del dominio de broadcast. La información de ruta se determina mediante la suma de los costos individuales de los puertos que atraviesa la ruta desde el destino al puente raíz. Si existe más de una ruta a escoger, el STA elige la de menor costo de ruta.

Los costos de los puertos predeterminados se definen por la velocidad a la que funcionan los mismos. El IEEE define los valores de costos de puertos utilizados por STP. Actualmente, debido al ingreso reciente al mercado de tecnologías Ethernet más veloces, los valores de costos de rutas pueden cambiar para ajustarse a las distintas velocidades disponibles.

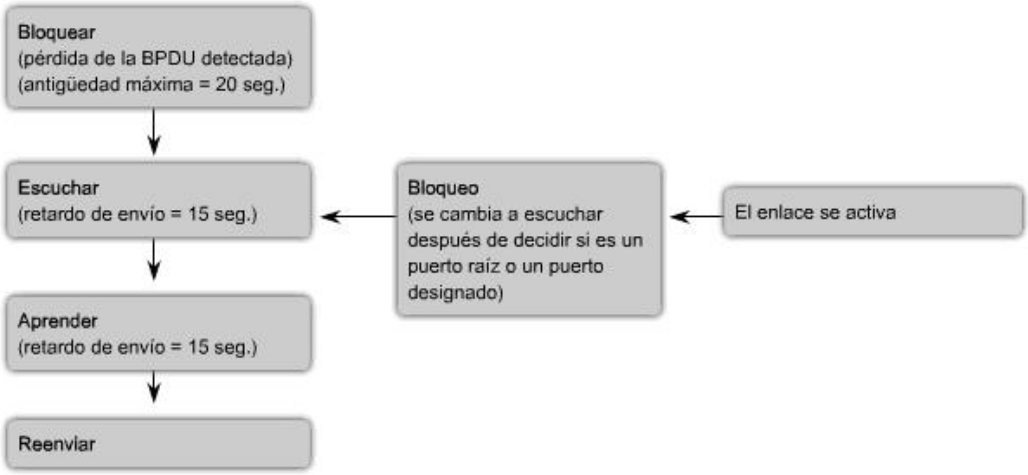
En la Tabla 3-24, los valores ya se han modificado para ajustarse al estándar Ethernet más reciente, observándose que los puertos Ethernet de 10 Gb/s poseen un costo de puerto de 2, los puertos Ethernet de 1 Gb/s poseen un costo de puerto de 4, los puertos Fast Ethernet de 100 Mb/s poseen un costo de puerto de 19 y los puertos Ethernet de 10 Mb/s poseen un costo de puerto de 100.

Velocidad de enlace	Costo (especificación IEEE revisada)	Costo (especificación IEEE anterior)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

Tabla 3-24 Las mejores rutas al puente raíz

Pese a que los puertos de switch cuentan con un costo de puerto predeterminado asociado a los mismos, tal costo puede configurarse. La capacidad para configurar los costos de puertos individuales proporciona al administrador la flexibilidad para controlar las rutas de spanning-tree hacia el puente raíz.

Los puertos pasan por cuatro estados: Bloquear, Escuchar, Aprender, y Reenviar. Un quinto estado, deshabilitado, indica que el administrador ha cerrado el puerto. Cuando se enciende un switch, en primer lugar, entra en un estado de bloqueo para impedir de inmediato la formación de un bucle. A continuación, cambia a modo de escucha, de modo que reciba BPDUs de los switches vecinos. Después de procesar esta información, el switch determina que puertos pueden estar activos. Si el puerto puede enviar tramas, cambia a modo de aprendizaje, y luego a modo de envío. Como consecuencia de este proceso, pueden llegar a transcurrir hasta 50 segundos mientras el puerto pasa por todos estos estados y queda listo para el envío de tramas.



	Bloquear	Escuchar	Aprender	Reenviar
Procesa BPDUs	✓	✓	✓	✓
Aprende direcciones MAC			✓	✓
Descarta tramas	✓			
Reenvía tramas				✓
No reenvía tramas	✓	✓	✓	
Recibe BDPUs	✓	✓	✓	✓
No aprende direcciones MAC	✓	✓		

Figura 3-33 Protocolo STP – Estados de los puertos

Cuando se desarrolló el estándar original, IEEE 802.1D Spanning Tree Protocol (STP), el tiempo de recuperación de 1 a 2 minutos, era aceptable. La necesidad de llevar tráfico sensible sin retardos, tales como voz y vídeo, requiere que las redes de conmutación converjan rápidamente para mantenerse al día con la nueva tecnología. Rapid Spanning Tree Protocol (RSTP), definida en IEEE 802.1w, acelera significativamente el cálculo del árbol de expansión.

RSTP requiere enlaces a full-duplex y conexiónes punto-a-punto entre los switches, para lograr mayor velocidad de reconfiguración. La reconfiguración del árbol de expansión por RSTP se produce en menos de 1 segundo, en comparación con los 50 segundos de STP.

Para acelerar el proceso de cálculo, RSTP reduce el número de estados del puerto a tres: Descarte, Aprendizaje y Reenvío. No posee estado de puerto bloqueado. El estado de descarte es similar a tres de los estados originales de STP (bloquear, escuchar, y deshabilitado).

Además RSTP introduce el concepto de la topología activa. Los puertos raíz y designado forman parte de la topología activa. Los puertos alternativo y de respaldo no están incluidos en la topología activa. Todos los puertos que no son del tipo descarte forman parte de dicha topología y de inmediato deben pasar al estado de envío.

Estado de puerto operativo	Estado del puerto en STP	Estado del puerto en RSTP
Habilitado	Bloquear	Descartar
Habilitado	Escuchar	Descartar
Habilitado	Aprender	Aprender
Habilitado	Reenviar	Reenviar
Deshabilitado	Deshabilitado	Descartar

Figura 3-34 STP vs. RSTP - Estados de los puertos

La función del puerto define el objetivo principal de un puerto de switch y la forma en que gestiona las tramas de datos. RSTP redefine el rol y estado de los puertos tal como muestra la siguiente tabla.

Puerto raíz	Existe en los puentes que no son raíz y es el puerto de switch con la mejor ruta hacia el puente raíz. Sólo se permite un puerto raíz por puente. El puerto raíz asume el estado de enviar en una topologia activa estable.
Puerto designado	Existen en los puentes raíz y en los que no son raíz. El puerto designado asume el estado de enviar. ▪ Para los puentes raíz, todos los puertos de switch son designados. ▪ Para los puentes que no son raíz, en una topología activa y estable, un

	puerto designado es el switch que recibe y envía tramas hacia el puente raíz según sea necesario. Sólo se permite un puerto designado por segmento.
Puerto alternativo	Puerto de switch que ofrece una ruta alternativa hacia el puente raíz. El puerto alternativo asume el estado de descarte en una topología activa estable. Un puerto alternativo estará presente en switches no designados y sufrirá la transición a puerto designado si el actual falla.
Puerto de respaldo	Existe en los puentes designados. Es un puerto de switch adicional con un enlace redundante al segmento para el cual el puente es designado. Un puerto de respaldo posee un ID de puerto mayor que el puerto designado, y asume el estado de descarte en una topología activa estable.

Tabla 3-25 Protocolo RSTP. Funciones de los puertos

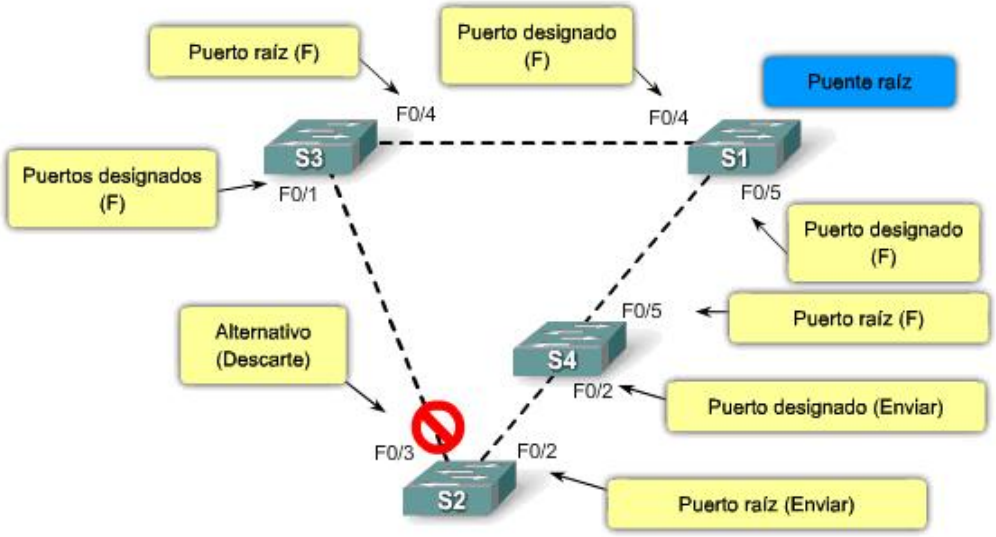


Figura 3-35 Protocolo RSTP – Ejemplo de funciones de los puertos

RSTP (802.1w) utiliza BPDU versión 2, pero sigue siendo compatible con STP (802.1D). RSTP envía BPDU cada 2 segundos, pero completa el byte señalizador de una manera ligeramente distinta al estándar 802.1D, como se aprecia en la Figura 3-36, reservando algunos bits para codificar la función y estado del puerto que origina la BPDU.

Campo	Longitud en bytes
ID de protocolo = 0x0000	2
ID de versión de protocolo = 0x02	1
Tipo de BPDU = 0x02	1
Señaladores	1
ID de raíz	8
Costo de la ruta raíz	4
ID de puente	8
ID del puerto	2
Antigüedad del mensaje	2
Antigüedad máxima	2
Tiempo de saludo	2
Retardo de envío	2

Bit del campo	Bit
Cambio en la topología	0
Propuesta	1
Función de puerto Puerto desconocido Puerto alternativo o de respaldo Puerto raíz Puerto designado	2-3 00 01 10 11
Aprender	4
Enviar	5
Acuerdo	6
Acuse de recibo de cambio de topología	7

Figura 3-36 Protocolo RSTP – Estructura BDPU versión 2

La información de protocolo puede expirar de forma inmediata en un puerto si no se reciben BDPU de configuración durante tres periodos de tiempo consecutivos, 6 segundos de manera predeterminada, o si expira el temporizador de antigüedad máxima. Debido a que las BPDUs se utilizan como un mecanismo de actividad, tres BPDU perdidas de forma consecutiva indican la pérdida de conectividad entre un puente y su raíz vecina o puente designado. La rápida expiración de la información permite que los fallos se detecten muy rápidamente.

Para la convergencia de la red RSTP utiliza un proceso de propuesta y acuerdo. En STP, una vez que el puerto era seleccionado para convertirse en puerto designado, debía esperar el equivalente a dos veces el retardo de envío antes de pasar al estado de enviar. RSTP agiliza el proceso de recálculo de forma significativa después de un cambio de topología, ya que converge enlace por enlace y no depende de que los temporizadores expiren para que los puertos experimenten la transición. Por este motivo, RSTP proporciona una convergencia mucho más rápida después de un fallo o durante el restablecimiento de un switch.

Para finalizar con este apartado, dado que en un diseño jerárquico, la redundancia se logra en las capas de distribución y núcleo, a través de hardware adicional y rutas alternativas entre dicho hardware, a continuación, se analiza un ejemplo en el que se observa una red jerárquica con capas de acceso, distribución y núcleo.

Cada switch de la capa de acceso se conecta a dos switches distintos de la capa de distribución. Además, cada switch de la capa de distribución se conecta a los dos switches de la capa núcleo. Al contar con varias rutas entre el PC1 y el PC4, existe redundancia que puede generar un único

punto de fallo entre las capas de acceso y distribución, y entre las capas de distribución y núcleo. Considerar STP habilitado en todos los switches y suponer que algunos puertos se encuentran en estado de enviar y otros en estado de bloqueo, para evitar bucles en la capa 2.

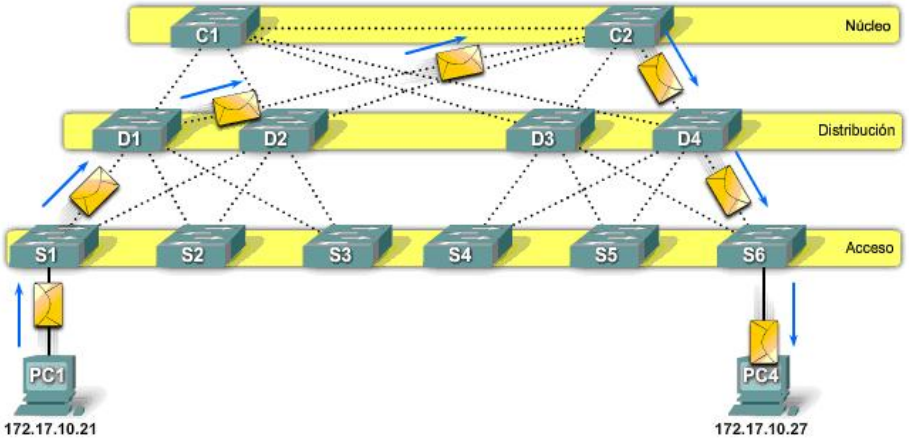


Figura 3-37 Diseño redundante. No fallo.

STP sólo utiliza un enlace redundante si existe un fallo en el enlace principal. En el ejemplo anterior, el PC1 puede comunicarse con el PC4 a través de la ruta identificada. Sin embargo, si falla la ruta de acceso a la capa de distribución o la ruta de distribución la situación sería la que muestra la Figura 3-38.

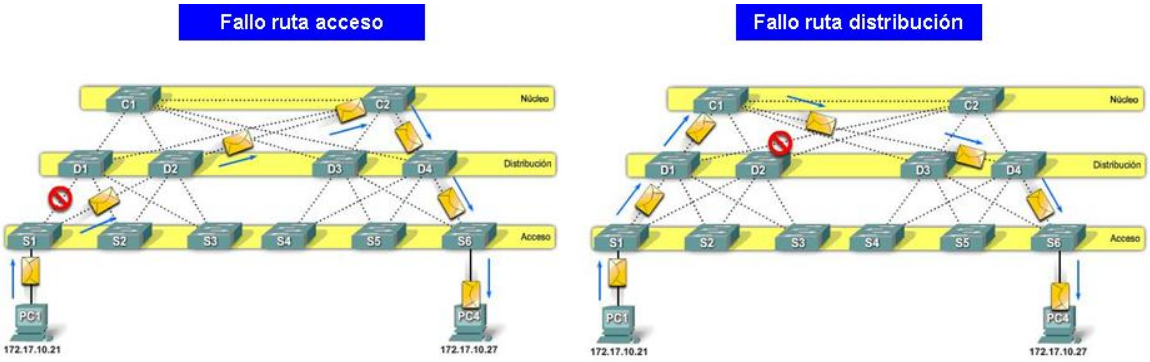


Figura 3-38 Diseño redundante. Fallos en rutas de acceso y distribución.

En ambos casos, existe un enlace interrumpido que impide que los datos del PC1 con destino el PC4 lleguen a través de su ruta original. Sin embargo, la existencia de una segunda ruta alternativa permite que dichos datos puedan alcanzar su destino.

En la imagen de la izquierda de la Figura 3-38 se observa un fallo en la ruta de acceso, ya que el enlace entre el switch S1 y el switch D1 se ha interrumpido. Sin embargo, en esta ocasión, el switch S1 cuenta con una segunda ruta al PC4 a través del switch D2. Por su parte, la imagen de la derecha presenta un fallo en la ruta de distribución, ya que el enlace entre el switch D1 y el

switch C2 se ha interrumpido, sin embargo, gracias a la redundancia, el switch D1 cuenta con una segunda ruta al PC4 a través del switch C1.

Los anteriores han sido fallos en los enlaces, a continuación, se examinan ejemplos de fallos en switches de la capa de distribución o de la capa núcleo.

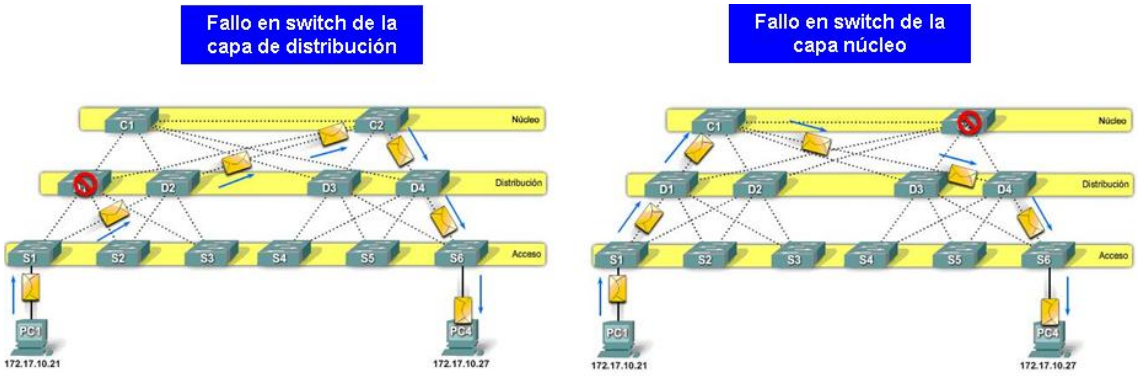


Figura 3-39 Diseño redundante. Fallos en switch de capa distribución y capa núcleo.

En ambos casos, existe un switch que ha fallado, por lo que los datos del PC1 no pueden llegar al PC4 a través de su ruta original. Sin embargo, una vez más, la existencia de una segunda ruta permite que dichos datos puedan alcanzar su destino.

En la imagen de la izquierda de la Figura 3-39, el switch de la capa de distribución D1 ha fallado. Sin embargo, el switch S1 cuenta con una segunda ruta al PC4 a través del switch D2. Por otro lado, la imagen de la derecha presenta un fallo en un switch de la capa núcleo, el C2. Sin embargo, el switch D1 cuenta con una segunda ruta al PC4 a través del switch C1.

Se llega a la conclusión, por tanto, de que la redundancia en los enlaces proporciona una gran flexibilidad en la elección de rutas de la red y permite que los datos se transmitan independientemente de la existencia de fallos en una sola ruta o en un dispositivo de las capas de distribución o núcleo, sin embargo, obliga a hacer uso de protocolos como Spanning Tree Protocol (STP) con el fin de evitar la aparición de bucles y tormentas de difusión en redes conmutadas.

3.10.2 Aplicación del STP al IATE

Con el fin de evitar que exista un único punto de fallo y tomando como referencia el modelo jerárquico, a nivel de capa de acceso se implementa redundancia en capa 2 mediante el uso del protocolo Rapid Spanning Tree (RSTP). Además para disponer de una ruta alternativa de tal modo que la red esté siempre en funcionamiento, se añaden enlaces redundantes desde el último switch hasta el primero tanto en Bilbao y O'Donnell, como en el Rack del Pasillo de SS.CC.

Figura 3-40 Redundancia en Bilbao – O'Donnell

En SS.CC, en la zona de servidores se utiliza EtherChannel con el fin de proporcionar tanto redundancia como velocidades mayores para el acceso a los servidores. Mientras que en el Centro de Procesamiento de Datos (CPD) a nivel de capa de acceso se implementan enlaces redundantes punto a punto con los switches de distribución/núcleo, y a nivel de capa de distribución/núcleo se implementa redundancia en capa 2 mediante el uso del protocolo RSTP. En el CPD también se utilizará EtherChannel para aumentar el ancho de banda y tener enlaces redundantes. Estas medidas van permitir tener siempre activa la VLAN de cada segmento, además de proporcionar balanceo de carga entre las VLANs.

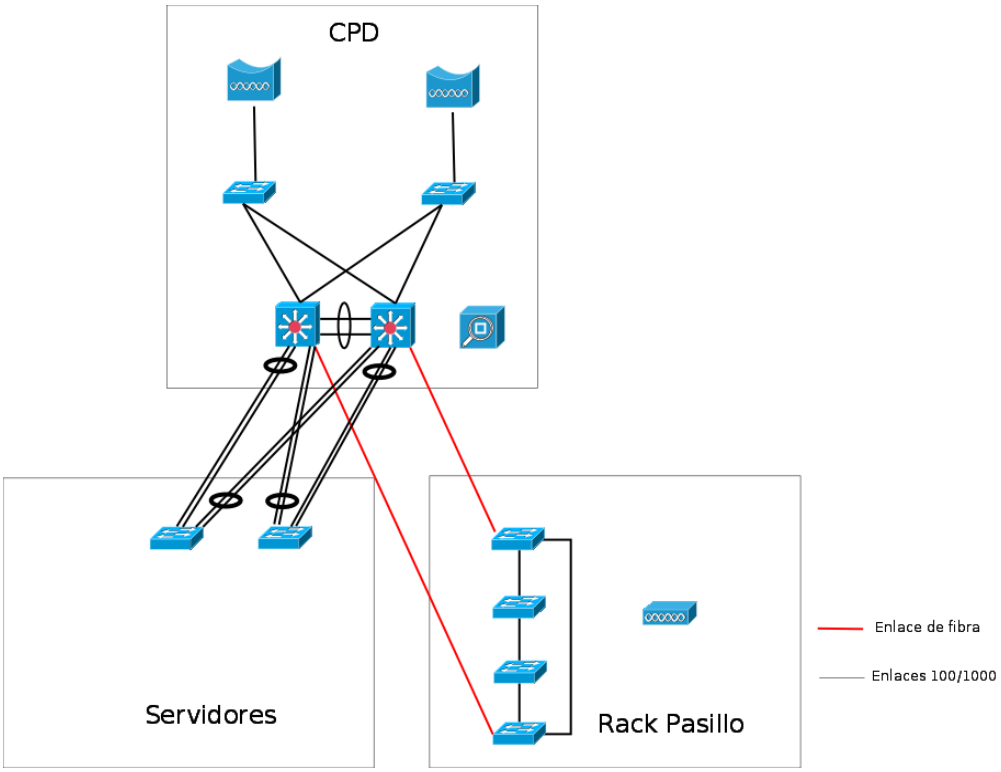


Figura 3-41 Redundancia en SS.CC.

A continuación se adjuntan una serie de listas de verificación que resumen los pasos seguidos para cumplir con los requisitos impuestos por el cliente en cuando a redundancia en capa 2.

Lista de verificación para Spanning Tree Protocol (STP)			
Requerimiento:		➢ **REQ_04**: El administrador de red debe asegurar una topología redundante para garantizar que la pérdida de servicio se mínima.	
Procedimiento:		Se implementa una topología física con bucles para tener rutas alternativas, y se utiliza RSTP para obtener una topología lógica libre de bucles a nivel de capa 2.	
Pasos		**Instrucciones**	**Referencias**
1	Seleccionar el puente raíz	No se permite que la decisión del puente raíz dependa de STP. Se coloca el puente raíz en el centro de la red, con una conexión directa a los servidores y routers. De este modo, se reduce la distancia promedio desde los clientes a los servidores y routers. En el IATE, los switch de la capa núcleo se han seleccionado como puente raíz. Al existir dos switches en la capa núcleo, uno actuará como principal y el otro como backup. Para conseguir el objetivo, se modifica las prioridades de los switches, el puente raíz toma prioridad 0 y el de backup prioridad 4096.	Figura 3-7 Arquitectura Lógica para el IATE
2	Seleccionar los puertos raíz	Todos los switches de un topología spanning-tree, excepto el puente raíz, poseen un único puerto raíz definido. El puerto raíz es el puerto de switch con el menor costo de ruta hacia el puente raíz.	Tabla 3-27 Las mejores rutas al puente raíz del IATE Figura 3-42 Diseño lógico con RSTP para el IATE
3	Seleccionar los puertos designados y no designados (Alternativo)	Cada segmento cuenta por lo menos con un puerto de switch designado para dicho segmento. En una topología activa y estable, el switch con el puerto designado recibirá tramas en el segmento con destino la puente raíz. El puerto alternativo asume el estado de descarte en una topología activa estable.	
4	Resolución de problemas	Fallo del enlace en la ruta hacia el núcleo	Figura 3-43 Fallo en la ruta al núcleo del IATE
		Fallo switch capa núcleo	Figura 3-44 Fallo en el switch núcleo del IATE

Tabla 3- 26 Lista de verificación para STP

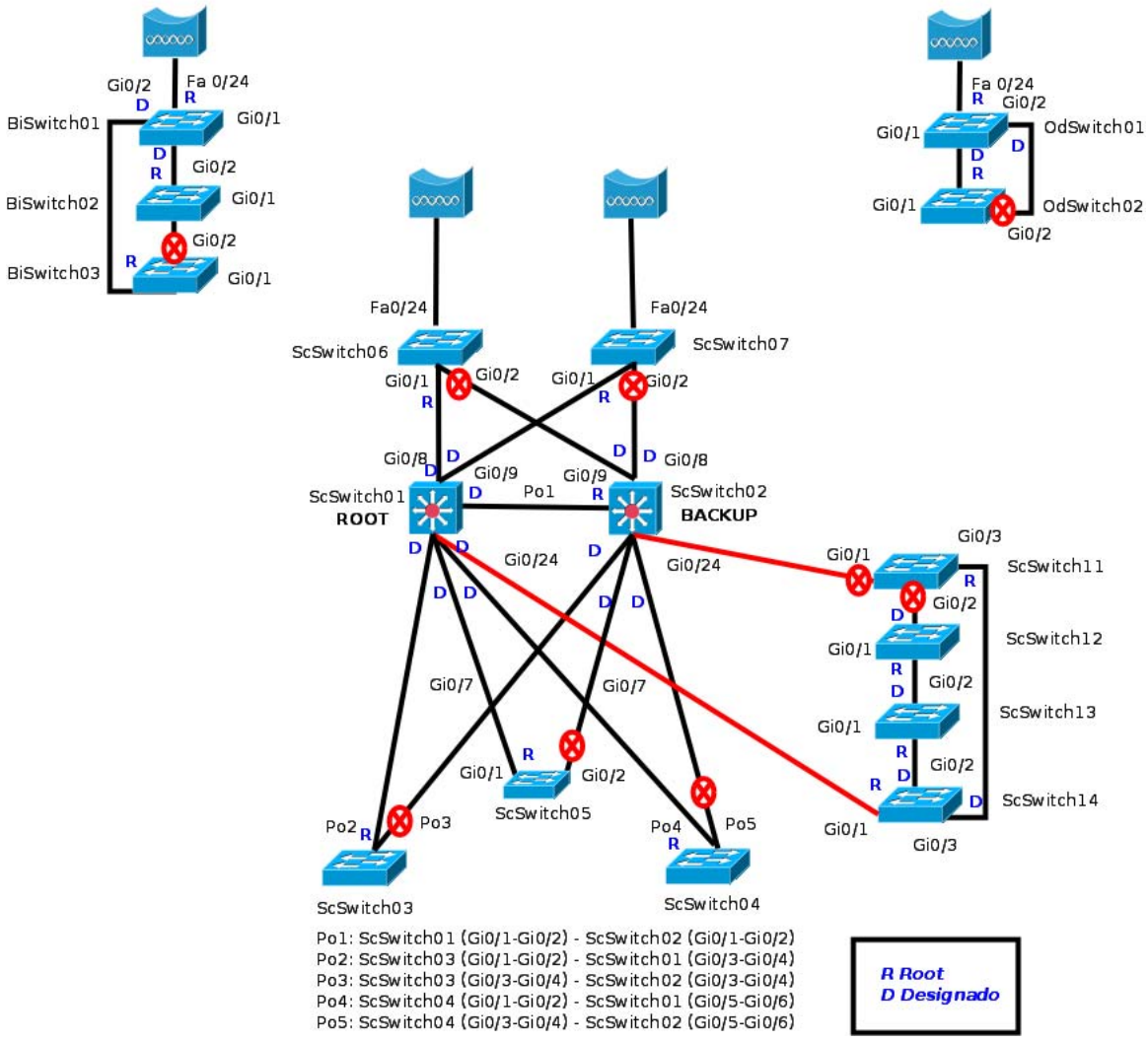


Figura 3-42 Diseño lógico con RSTP para el IATE

Switch	Puente Raíz	Puente Backup	Interfaz	Switch vecino	Rol	Estado	Costo de la ruta al raíz
Scswitch01	Scswitch01	ScSwitch02	Po1	ScSwitch02	Designado	Envío	-
			Po2	ScSwitch03	Designado	Envío	-
			Po4	ScSwitch04	Designado	Envío	-
			Gi0/7	ScSwitch05	Designado	Envío	-
			Gi0/8	ScSwitch06	Designado	Envío	-
			Gi0/9	ScSwitch07	Designado	Envío	-
			Gi0/24	ScSwitch14	Designado	Envío	
ScSwitch02	Scswitch01	ScSwitch02	Po1	Scswitch01	**Root**	Envío	**3**
			Po3	ScSwitch03	Designado	Envío	-
			Po5	ScSwitch04	Designado	Envío	-
			Gi0/7	ScSwitch05	Designado	Envío	
			Gi0/8	ScSwitch07	Designado	Envío	-
			Gi0/9	ScSwitch06	Designado	Envío	-
			Gi0/24	ScSwitch11	Designado	Envío	-
ScSwitch03	Scswitch01	ScSwitch02	Po2	Scswitch01	**Root**	Envío	**3**
			Po3	ScSwitch02	Alternativo	Bloqueado	-
ScSwitch04	Scswitch01	ScSwitch02	Po4	Scswitch01	**Root**	Envío	**3**
			Po5	ScSwitch02	Alternativo	Bloqueado	-
ScSwitch05	Scswitch01	ScSwitch02	Gi0/1	Scswitch01	**Root**	Envío	**4**
			Gi0/2	ScSwitch02	Alternativo	Bloqueado	-
ScSwitch06	Scswitch01	ScSwitch02	Gi0/1	Scswitch01	**Root**	Envío	**4**
			Gi0/2	ScSwitch02	Alternativo	Bloqueado	-
			Fa0/24	BiSwitch01	Designado	Envío	-
ScSwitch07	Scswitch01	ScSwitch02	Gi0/1	Scswitch01	**Root**	Envío	**4**
			Gi0/2	ScSwitch02	Alternativo	Bloqueado	-

Switch	Puente Raíz	Puente Backup	Interfaz	Switch vecino	Rol	Estado	Costo de la ruta al raíz
			Fa0/24	OdSwitch01	Designado	Envío	-
ScSwitch11	Scswitch01	ScSwitch02	Gi0/1	ScSwitch02	Alternativo	Bloqueado	-
			Gi0/2	ScSwitch12	Alternativo	Bloqueado	-
			Gi0/3	ScSwitch14	**Root**	Envío	**8**
ScSwitch12	Scswitch01	ScSwitch02	Gi0/1	ScSwitch11	Designado	Envío	-
			Gi0/2	ScSwitch13	Root	Envío	-
ScSwtich13	Scswitch01	ScSwitch02	Gi0/1	ScSwitch13	Designado	Envío	-
			Gi0/2	ScSwitch14	**Root**	Envío	**8**
ScSwitch14	Scswitch01	ScSwitch02	Gi0/1	ScSwitch01	**Root**	Envío	**4**
			Gi0/2	ScSwitch13	Designado	Envío	-
			Gi0/3	ScSwitch11	Designado	Envío	-
BiSwitch01	Scswitch01	ScSwitch02	Fa0/24	ScSwitch06	**Root**	Envío	**23**
			Gi0/1	BiSwitch02	Designado	Envío	-
			Gi0/2	BiSwitch03	Designado	Envío	-
BiSwitch02	Scswitch01	ScSwitch02	Gi0/1	BiSwitch03	Designado	Envío	-
			Gi0/2	BiSwitch01	**Root**	Envío	**27**
BiSwitch03	Scswitch01	ScSwitch02	Gi0/1	BiSwitch01	**Root**	Envío	**27**
			Gi0/2	BiSwitch02	Alternativo	Bloqueado	-
OdSwitch01	Scswitch01	ScSwitch02	Fa0/24	ScSwitch07	**Root**	Envío	**23**
			Gi0/1	OdSwitch02	Designado	Envío	
			Gi0/2	OdSwitch02	Designado	Envío	
OdSwitch02	Scswitch01	ScSwitch02	Gi0/1	OdSwitch01	**Root**	Envío	**27**
			Gi0/2	OdSwitch02	Alternativo	Bloqueado	-

Tabla 3-27 Las mejores rutas al puente raíz del IATE

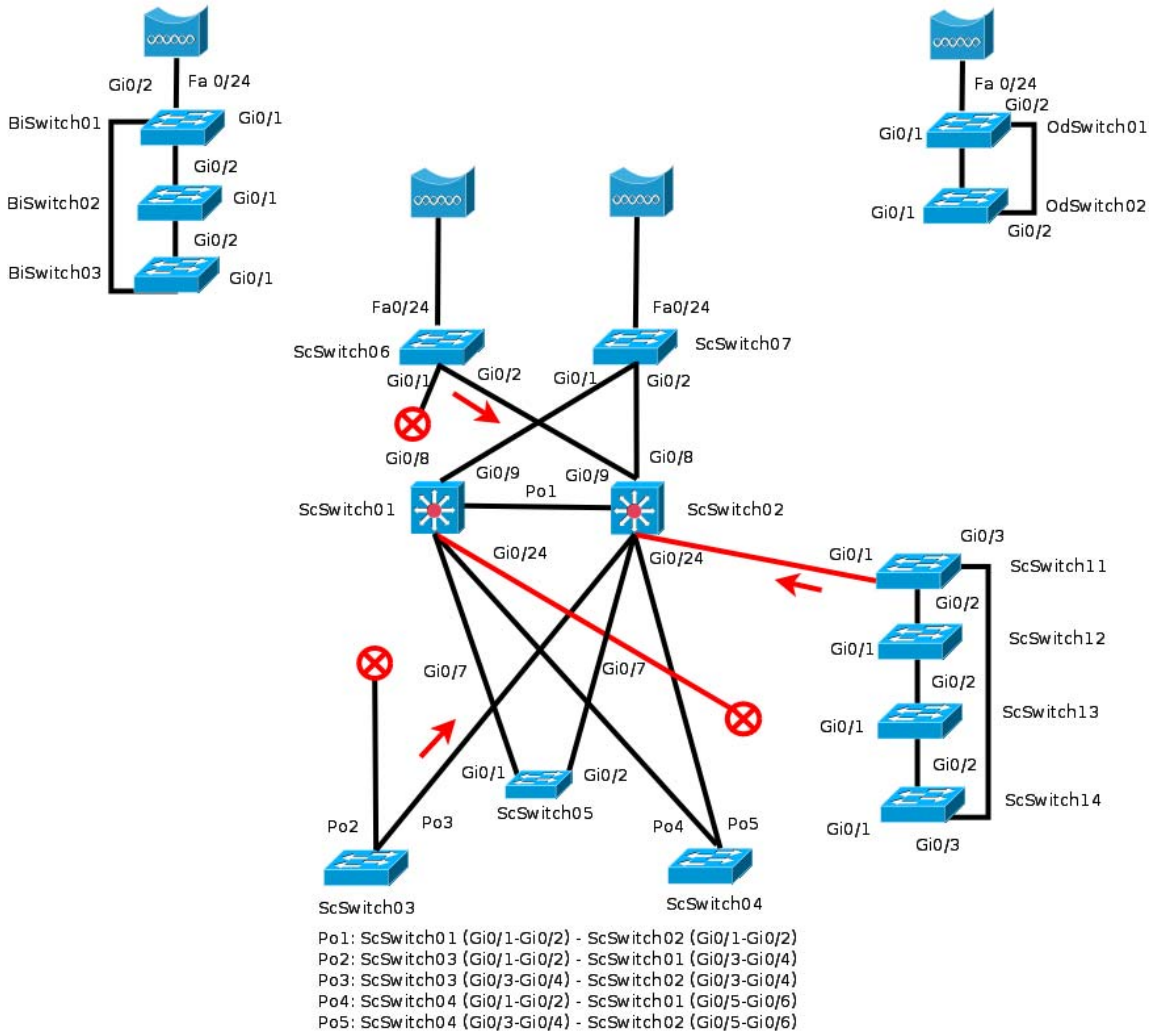


Figura 3-43 Fallo en la ruta al núcleo del IATE

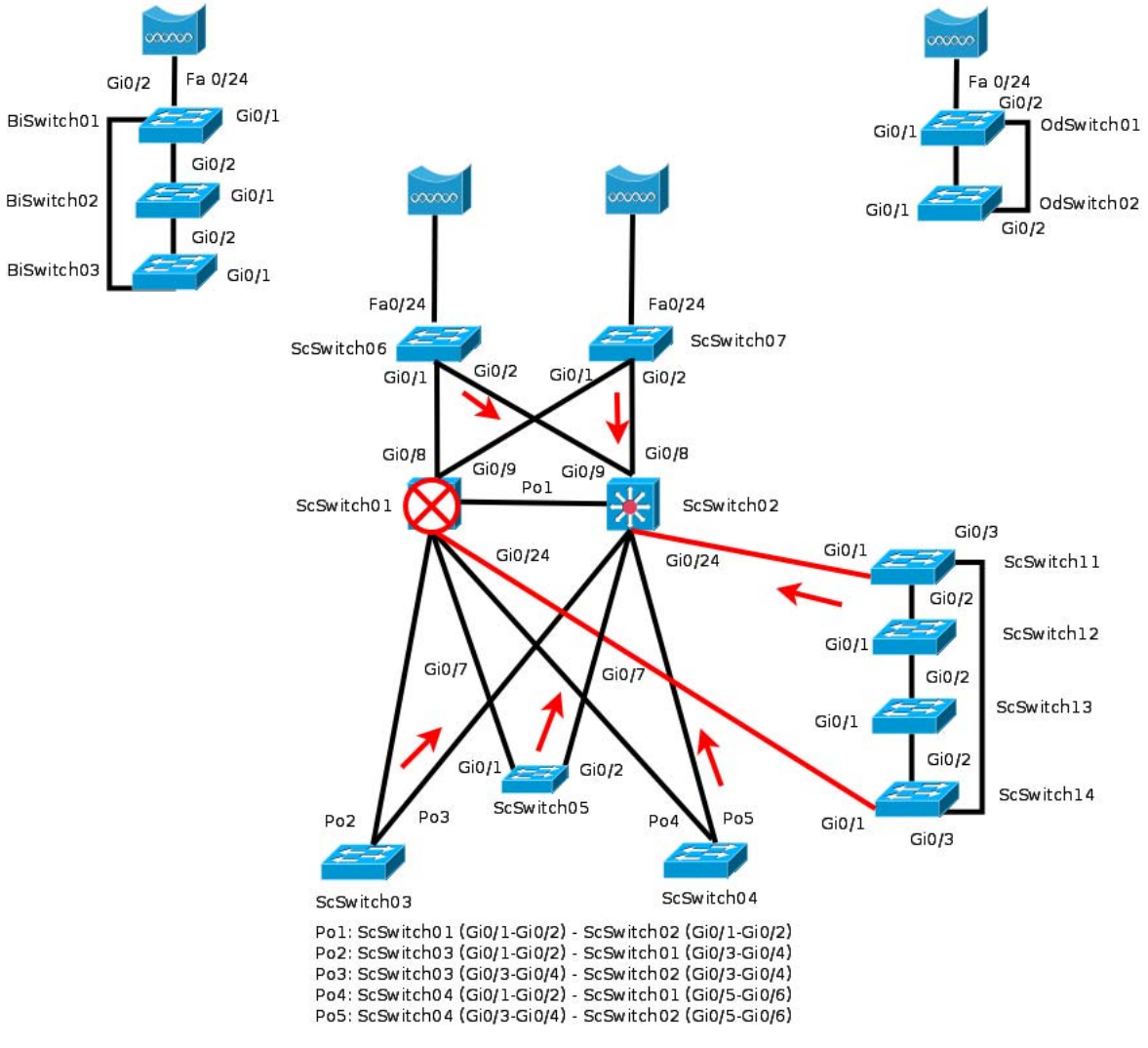


Figura 3-44 Fallo en el switch núcleo del IATE

3.10.3 Redundancia Capa 3 – Protocolo HSRP

Cuando una puerta de enlace predeterminada está configurada en un dispositivo, generalmente, no hay medios para configurar una puerta secundaria, aunque existe una segunda ruta para llevar los paquetes fuera del segmento local.

En la figura, el router A es el responsable del enrutamiento de los paquetes para la subred A, y el router B es el responsable del envío de paquetes para la subred B. Si el router A no está disponible, los protocolos de enrutamiento de forma rápida y dinámica convergen y determinan que el router B ahora puede transferir paquetes que antes han pasado por router A. Sin embargo, la mayoría de estaciones de trabajo, servidores e impresoras, no reciben esta información de enrutamiento dinámico.

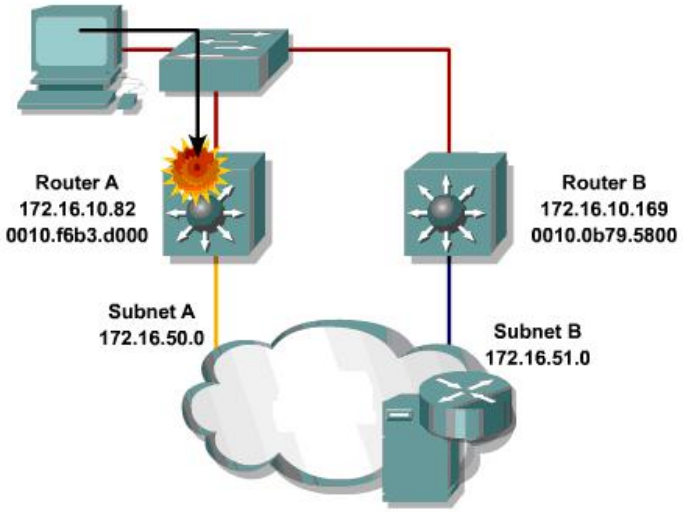


Figura 3-45 No Redundancia en capa 3

Los dispositivos finales suelen ser configurados con una única puerta de enlace predeterminada que no cambia cuando se producen cambios en la topología de la red. Por tanto, si no funciona el router cuya dirección IP se configura como puerta de enlace predeterminada, el dispositivo local no es capaz de enviar paquetes fuera del segmento de red local, de manera que pierde conectividad con el resto de la red. Incluso aunque existiese un router redundante que pudiera servir de puerta de enlace predeterminada para este segmento, no existe un método dinámico que permita a estos dispositivos determinar la dirección de una nueva puerta de entrada.

Para solucionarlo se puede usar redundancia en capa 3 con **Hot Standby Router Protocol (HSRP).** Con este tipo de redundancia un conjunto de routers, que comparten una dirección IP y una dirección MAC (capa 2), actúan como un único router virtual para las máquinas de la LAN. A este conjunto de routers se le denomina grupo HSRP. Este protocolo está diseñado para

segmentos LAN donde hay una gran cantidad de routers y dispositivos que utilizan solamente una dirección IP estática de la puerta de enlace predeterminada.

La dirección IP del router virtual se configura como puerta de enlace predeterminada para los puestos de trabajo en un segmento de IP específico. Las tramas son enviadas desde la estación de trabajo a la puerta de enlace predeterminada, ya que la estación de trabajo utiliza ARP para resolver la dirección MAC asociada con la dirección IP del router virtual.

El protocolo HSRP proporciona redundancia, y determina que router tomara el rol de activo para el envío de tráfico y cuando debe asumir el rol de pasivo. A intervalos regulares, los routers intercambian información para determinar cuales de ellos siguen estando presentes y son capaces de reenviar tráfico. La transición de router activo a pasivo es transparente para los dispositivos finales.

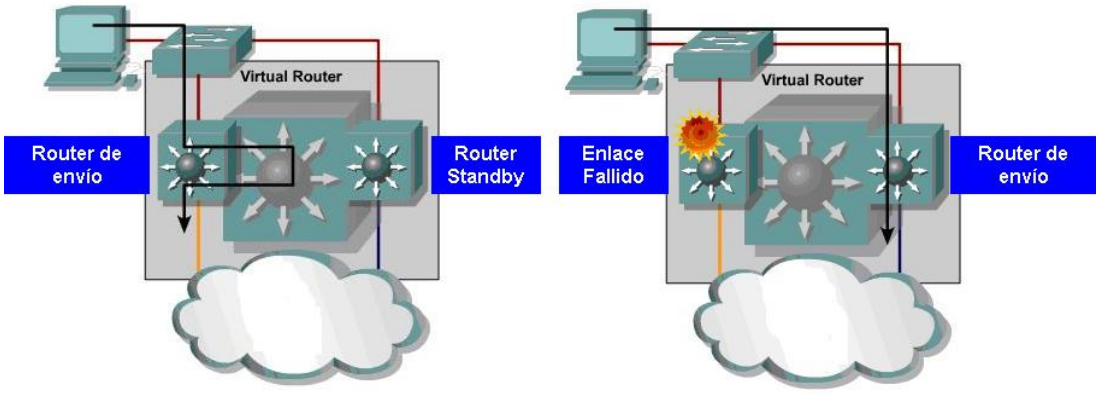


Figura 3-46 Redundancia Capa 3 – Router Virtual

Si falla el router principal de un grupo de routers con HSRP, hay un router de reserva en el mismo grupo que empieza a reenviar el tráfico. Dado que los routers deciden por si mismos cuál reenvía el trafico a la dirección virtual y dado que las estaciones de trabajo de un segmento sólo conocen la dirección IP virtual como su puerta de enlace predeterminada, un fallo del router de reenvío principal es prácticamente indetectable por parte de los usuarios de estaciones de trabajo y no requiere intervención por parte del usuario ni del administrador de red.

El router activo responde al tráfico enviado al router virtual y físicamente reenvía los paquetes enviados a la dirección MAC del router virtual. Si una estación final envía un paquete a la dirección MAC del router virtual, el router activo recibe y procesa ese paquete. Si una estación final envía una solicitud ARP con la dirección IP del router virtual, el router activo responde con la dirección MAC del router virtual. La dirección IP y la MAC correspondiente del router virtual se mantienen en la tabla ARP de cada router en el grupo HSRP.

En el siguiente ejemplo, el router A asume el papel activo y envía las tramas que se dirigen a la conocida dirección MAC de 0000.0c07.acxx, donde xx es el identificador de grupo HSRP. La figura describe también la salida del comando show arp ip para el grupo HSRP.

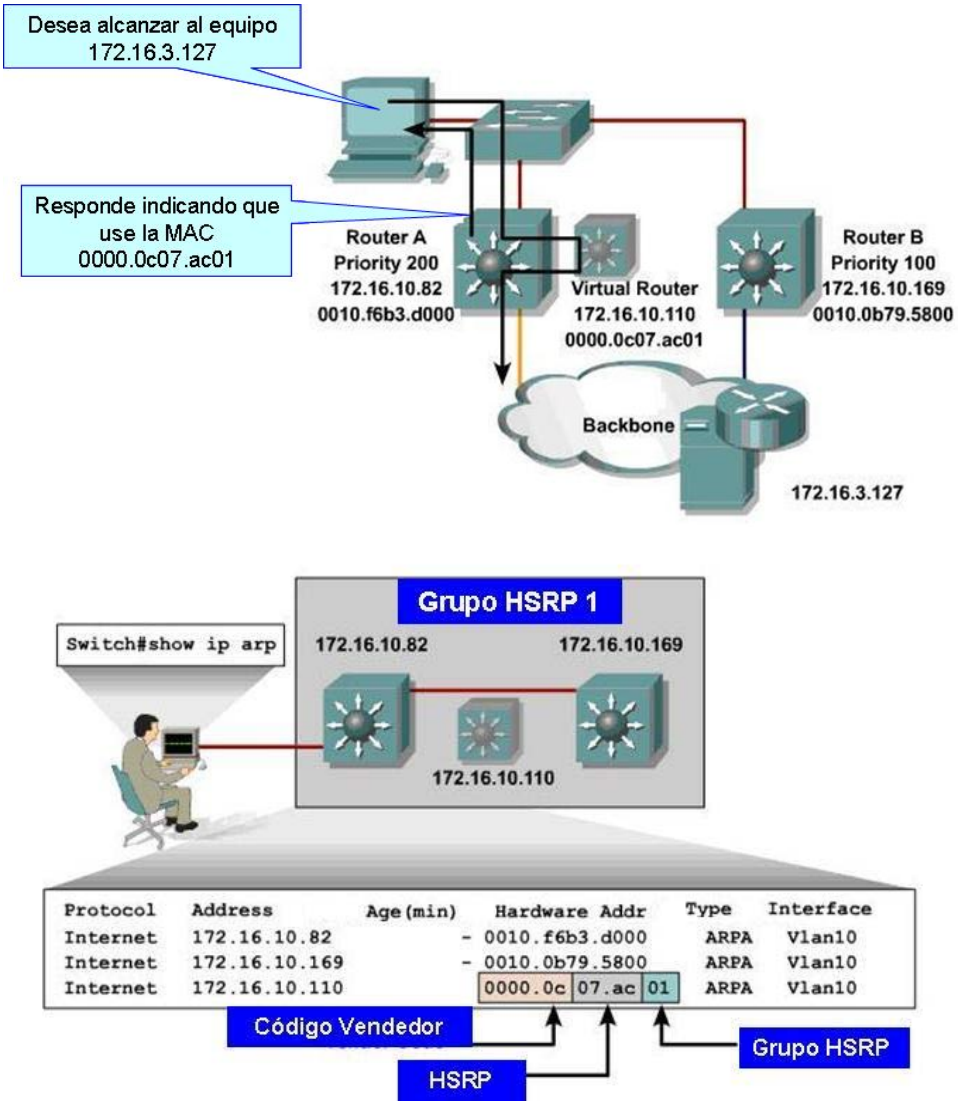


Figura 3-47 Redundancia Capa 3 – Grupo HSRP

Ambos routers, el activo y el que está en standby, intercambian mensajes, concretamente del tipo HSRP hello, que le permiten a cada uno conocer el estado del otro. Estos mensajes utilizan la dirección multicast 224.0.0.2 y el puerto UDP 1985.

Si el router activo no envía mensajes de tipo hello al router en standby dentro de un determinado periodo de tiempo, el router en standby asume que el activo está fuera de servicio y se convierte en activo. La conversión a router activo consiste en que uno de los router que actuaba como respaldo obtiene la dirección virtual que identifica al grupo de routers.

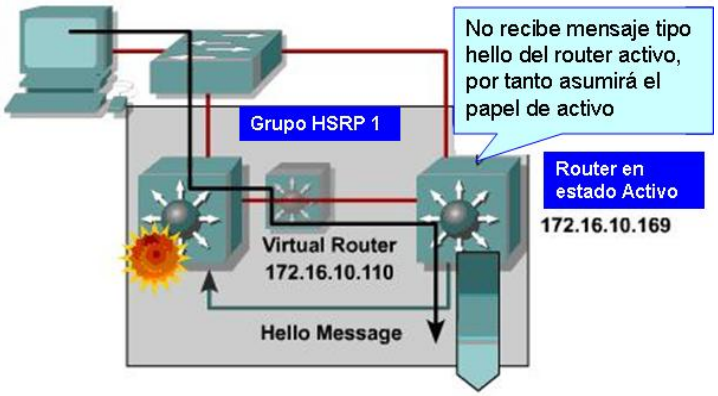


Figura 3-48 Transición a Router Activo

Algunos términos relacionados con los mensajes tipo hello son:

- **Hello Interval Time**: Intervalo de tiempo entre sucesivos mensajes tipo hello desde un router dado. Por defecto son 3 segundos.

- **Hold Interval Time**: Intervalo de tiempo entre la recepción de un mensaje tipo hello y la suposición de que el router que lo envía ha fallado, por tanto, es el tiempo durante el cual el actual mensaje hello se considera válido Por defecto son 10 segundos, lo que significa que el tiempo de conmutación por error puede ser de hasta 10 segundos para que los clientes empiecen a comunicarse con el gateway por defecto. En algunos casos, este intervalo puede ser excesivo para soporte de aplicaciones. El hold time debe ser de al menos tres veces el valor del tiempo de Hello.

Un router en un grupo HSRP puede estar en uno de los siguientes estados:

- **Initial**: Es el estado inicial e indica que HSRP no está funcionando. A este estado se entra a través de un cambio de configuración, cuando un interfaz arranca por primera vez o bien cuando el router no puede encaminar los paquetes a las direcciones IP que se le indican.

- **Learn**: Después del estado initial, la interfaz pasa al estado de learn, esperando ver paquetes HSRP y de estos paquetes determinar la dirección IP virtual y el router HSRP activo para el grupo. El router no tiene configurada la dirección IP virtual, y todavía no ha recibido un mensaje Hello autenticado del router activo. Espera recibir noticias del router activo. Todavía no tiene suficiente información como para intentar reclamar el papel de router activo o en standby.

- **Listen**: Una vez que la interfaz ha visto los paquetes HSRP y determinó la IP virtual, se mueve al estado de listen El router tiene configurada la dirección IP virtual, pero no es ni el router activo ni el de standby. Está a la escucha de mensajes Hello de esos routers.

Si los routers activo y en standby están funcionales, la interfaz sigue estando en este estado. Sin embargo, si no se ven tipo hello desde cualquiera de los dos routers, la interfaz pasa al estado de speak.

- **Speak**: El router envía mensajes Hello periódicamente y está participando activamente en la elección del router activo y/o de standby.

- **Standby**: El router standby es el candidato a convertirse en el siguiente router activo y envía mensajes Hello periódicamente. Excluyendo condiciones transitorias, debe haber como máximo un router en el grupo en estado standby.

- **Active**: El router está actualmente encaminando los paquetes enviados a la dirección MAC virtual del grupo HSRP. Envía mensajes Hello periódicamente. Excluyendo situaciones transitorias, sólo puede haber un router en estado activo en todo el grupo.

HSRP posee opciones de optimización entre las que se encuentran los temporizadores, la prioridad en standby, la opción standby preempt y el tracking. Cada una de estas características se detallará a continuación.

Cada router mantiene tres temporizadores, el active timer, el standby timer y el hello timer. El active timer se utiliza para controlar al router activo y se restablece cada vez que un router en el grupo recibe un paquete hello desde el router activo, mientras que el standby timer se utiliza para controlar al router en standby y se restablece cada vez que un router en el grupo recibe un paquete hello desde el router en standby. Ambos temporizadores expiran, de conformidad con el valor de hold time, establecido en el campo correspondiente del mensaje hello.

En cambio el hello timer se utiliza para controlar los paquetes hello. Todos los routers en el grupo, en cualquier estado HSRP, generan un paquete hello cuando este temporziador expira. La reducción del temporizador hello puede provocar el aumento del tráfico de mensajes de hello y debe usarse con cautela.

Por su parte, la opcion Standby Priority permite al administrador de red controlar el orden en el cual se seleccionarán los routers activos en el grupo. Durante el proceso de selección, el router con la más alta prioridad en un grupo HSRP se convierte en el router activo. En el caso de un empate, se elige el router con la más alta dirección IP configurada.

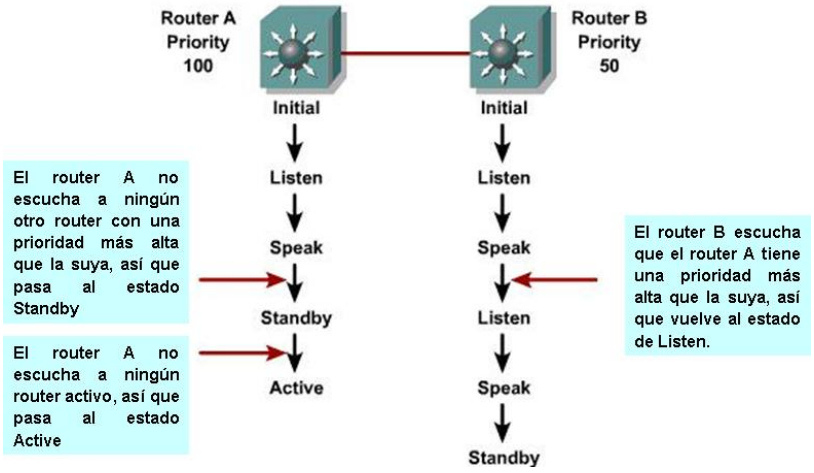


Figura 3-49 Protocolo HSRP. Estado de los routers del grupo

Como se ha descrito anteriormente, el router en standby asume automáticamente la función de router activo cuando el router activo falla o se retira del servicio. Este nuevo router activo, es el encargado del reenvío de paquetes, incluso si un router con más alta prioridad entra en servicio en la red o aunque el router activo que se había caído vuelva a levantarse. Este funcionamiento, además, ocasiona que un router que arranca más rápido que los demás en el grupo se convierta en router activo, independientemente de la prioridad configurada.

Para solventar estas situaciones, la interfaz del router se puede configurar con el comando standby preempt, ya que esta opción le permite tomar el rol de activo incluso aunque exista otro router activo en el grupo.

Para concluir queda tratar otra de las técnicas avanzadas de HSRP como es el Tracking, para lo cual se va a comenzar analizando los problemas que pueden surgir en el caso de existan dos o mas rutas diferentes para el acceso a los recursos de una red.

A modo de ejemplo suponer que 2 routers, A y B, residen en un edificio, y cada uno de ellos dispone de un enlace Gigabit Ethernet al otro edificio. El router A tiene la mayor prioridad y es el router activo para el Grupo HSRP 1, mientras que el router B es el router en standby. Ambos están intercambiando mensajes tipo Hello a través de sus interfaces E0.

Si el enlace Gigabit Ethernet entre el router activo y la sede experimenta un fallo y el protocolo HSRP no está habilitado, el router A no puede detectar el fallo del enlace. Por lo tanto, aunque la interfaz del G1 con el router A ya no es funcional, éste todavía comunica mensajes Hello por la interfaz E0, por lo que sigue siendo el router activo, sin embargo, los paquetes enviados al router virtual para su transmisión a la sede no pueden ser enviados porque el enlace que da acceso a dicha sede ha experimentado un fallo.

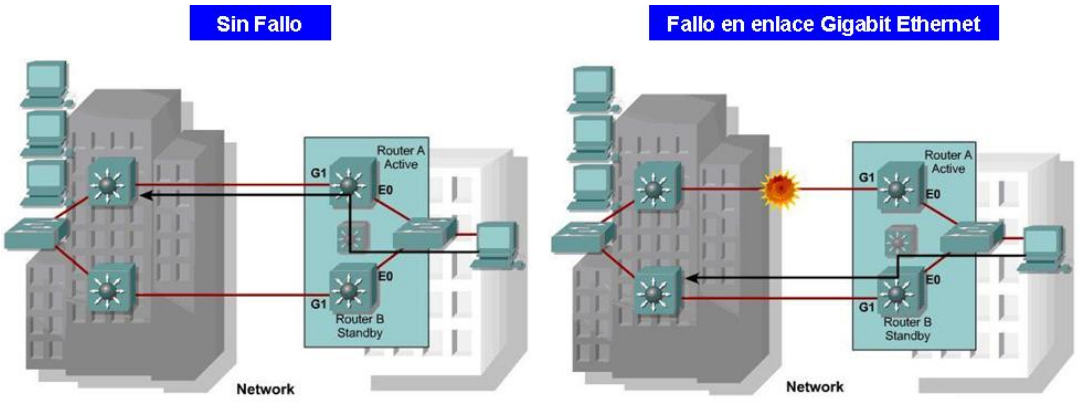


Figura 3-50 Dos rutas diferentes para el acceso a los recursos de red

Una alternativa para solventar esta situación sería que un protocolo de enrutamiento dinámico (si está en uso) detecte el fallo de un enlace y actualice las tablas de enrutamiento de los routers. Aún así, el tráfico sería enviado por los hosts al router activo y éste tendría que enviarlos de vuelta a través del segmento Ethernet al router en standby, donde el enlace Gigabit podría ser utilizado.

Cuando una interfaz tracked no está disponible, se reduce la prioridad HSRP del router afectado. De esta manera, se consigue que un router con una interfaz clave no disponible, renuncie a la función de router activo.

Aplicando la opción de tracking al ejemplo de la Figura 3-50, el router A configura la interfaz G1 como tracked. Si el enlace entre la interfaz del G1 y el otro edificio falla, el router automáticamente disminuye la prioridad de la interfaz E0 y dejará de transmitir mensajes hello sobre la interfaz. Transcurrido el intervalo de Hold Time sin detectar mensajes tipo hello del router A, el router B asume la función de router activo.

HSRP permite ser utilizado para balancear la carga, sacando, de este modo, ventaja a la existencia de múltiples rutas hacia un mismo destino. Con un único grupo HSRP en una subred, el router activo es el que reenvía todos los paquetes fuera de la subred, mientras que el router en standby no reenvía ningún paquete. Para facilitar el balanceo de carga, un router puede ser miembro de varios grupos HSRP en el mismo segmento.

Cada grupo HSRP emula un router virtual pero un mismo router puede pertenecer a distintos grupos e incluso estar en un estado diferente para cada grupo, es decir, puede actuar como activo en un grupo HSRP y al mismo tiempo estar en estado standby en otro grupo. Sin embargo, aumentar el número de grupos en los que participa un router aumenta la carga en dicho router, por lo que puede afectar a su rendimiento.

En la Figura 3-51, tanto el router A como el B son miembros de los Grupos 1 y 2. El router A está activo para el Grupo 1 y en standby para el Grupo 2, mientras que el router B es el activo para el Grupo 2 y el router en standby para el Grupo 1.

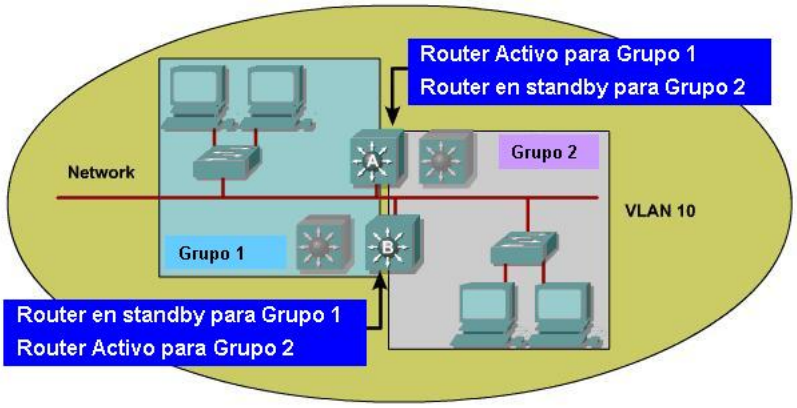


Figura 3-51 Routers compartidos entre varios grupos HSPR

Por tanto, varios routers, que se configuran como interfaces VLAN, pueden al mismo tiempo proporcionar redundancia, eliminando situaciones en las que un único punto de fallo provoque interrupciones de tráfico, y balanceo de carga a través de diferentes subredes IP.

3.10.4 Aplicación del HSRP al IATE

En el Centro de Procesamiento de Datos (CPD) de SS.CC., a nivel de capa de distribución/núcleo, se implementa redundancia en capa 3 a través del protocolo HSRP

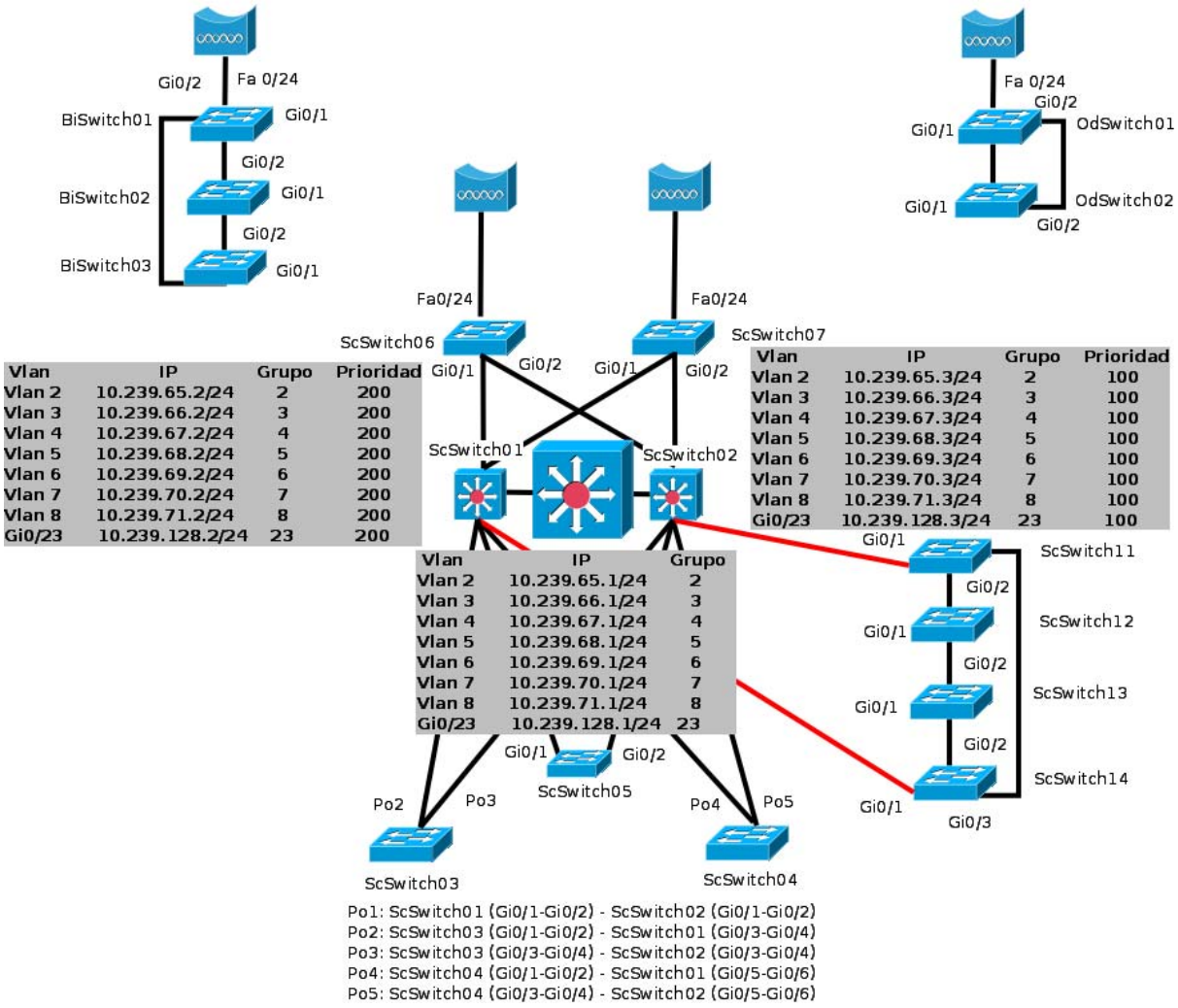
A continuación se adjuntan una serie de listas de verificación que resumen los pasos seguidos para cumplir con los requisitos impuestos por el cliente en cuando a redundancia en capa 3.

Lista de verificación para Hot Standby Router Protocol (HSRP)			
Requerimiento:		➢ **REQ_06**: El administrador debe garantizar el acceso a los servidores y la salida al exterior, para evitar perdidas de servicio	
Procedimiento:		Se utiliza HSRP para proporcionar rutas a alternativas a nivel de capa 3	
Pasos		**Instrucciones**	**Referencias**
1	Asignación de IP a las interfaces virtuales del switch principal	No se requieren	Figura 3-52 Direccionamiento Switch capa núcleo del IATE Tabla 3-29 Direccionamiento Switch capa núcleo del IATE
2	Asignación de IP a las interfaces virtuales del switch backup	No se requieren	
3	Asignación de IP HSRP tanto al switch principal como de backup	No se requieren	
4	Asignación de prioridad	El switch con prioridad mayor toma el rol activo, en este caso el ScSwitch01, al que se le asigna prioridad 200. Al switch de backup se le asigna la que viene por defecto, 100, tomando el rol de pasivo.	
5	El router principal siempre debe ser el router activo	Para lógralo se utiliza en la configuración la opción preempt, que permite que el router principal tome el rol de activo incluso aunque exista otro router activo.	
6	Uso de interfaz de tracking.	Permite controlar una determinada interfaz del switch para el proceso de HSRP, a fin de alterar la prioridad HSRP de un grupo determinado si esta interfaz cae. En el caso del IATE se controla la interfaz Gigabit 0/24, si ésta cae se disminuye la prioridad del switch a 150.	Figura 3-53 Interfaz Tracking para Switch Activo del IATE
7	Resolución de problemas	Caída del switch principal	Figura 3-44 Fallo en el switch núcleo del IATE
		Caída de la Interfaz tracking	Figura 3-54 Caída Interfaz Tracking en Switch Activo

Tabla 3-28 Lista de verificación para HSRP

Interfaz Virtual	IP HSPR	Grupo	Switch	IP Switch	Prioridad Switch
Vlan 2	10.239.65.1/24	2	ScSwitch01	10.239.65.2/24	200
			ScSwitch02	10.239.65.3/24	100
Vlan 3	10.239.66.1/24	3	ScSwitch01	10.239.66.2/24	200
			ScSwitch02	10.239.66.3/24	100
Vlan 4	10.239.67.1/24	4	ScSwitch01	10.239.67.2/24	200
			ScSwitch02	10.239.67.3/24	100
Vlan 5	10.239.68.1/24	5	ScSwitch01	10.239.68.2/24	200
			ScSwitch02	10.239.68.3/24	100
Vlan 6	10.239.69.1/24	6	ScSwitch01	10.239.69.2/24	200
			ScSwitch02	10.239.69.3/24	100
Vlan 7	10.239.70.1/24	7	ScSwitch01	10.239.70.2/24	200
			ScSwitch02	10.239.70.3/24	100
Vlan 8	10.239.71.1/24	8	ScSwitch01	10.239.71.2/24	200
			ScSwitch02	10.239.71.3/24	100

Tabla 3-29 Direccionamiento Switch capa núcleo del IATE

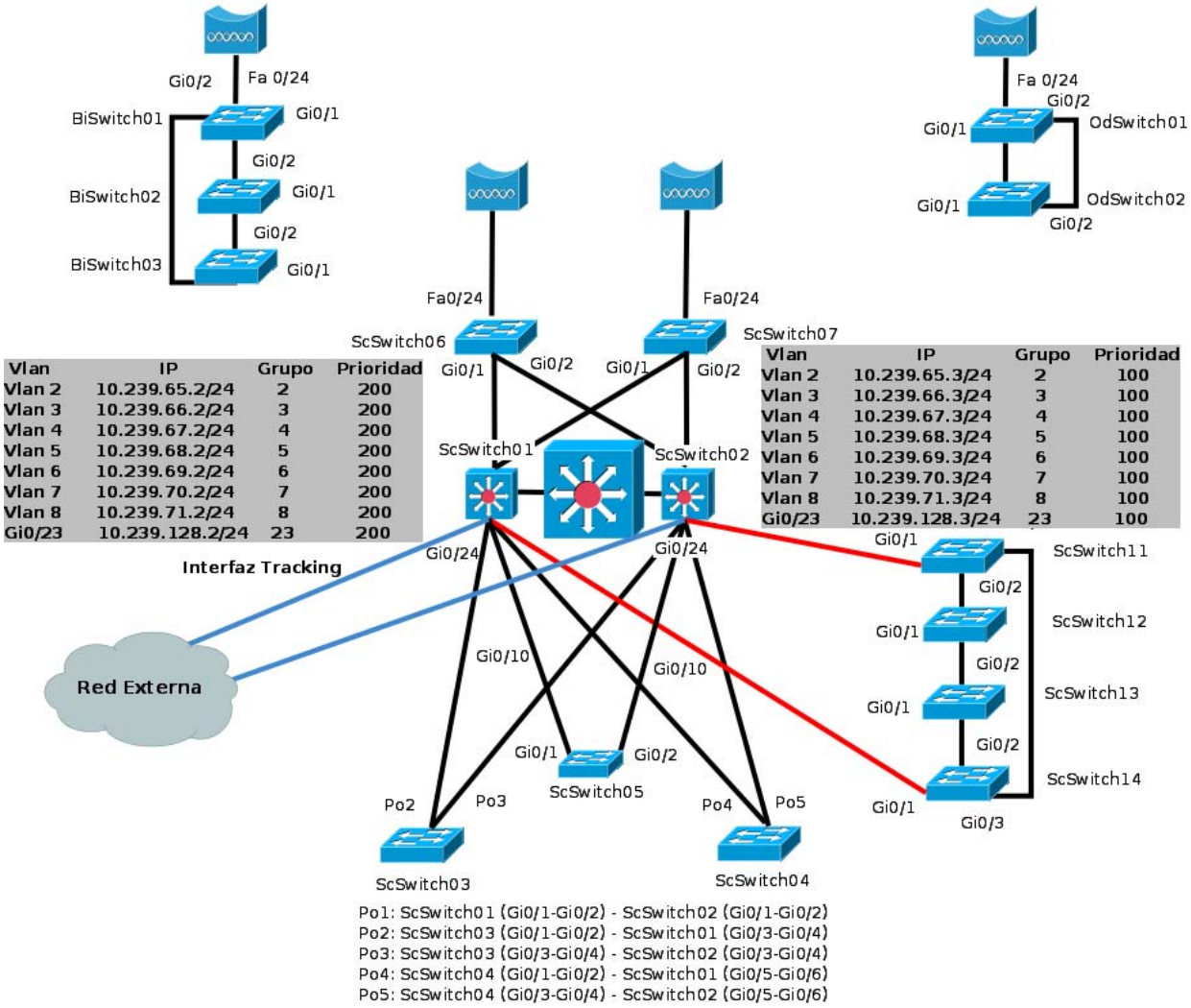


Vlan	IP	Grupo	Prioridad
Vlan 2	10.239.65.2/24	2	200
Vlan 3	10.239.66.2/24	3	200
Vlan 4	10.239.67.2/24	4	200
Vlan 5	10.239.68.2/24	5	200
Vlan 6	10.239.69.2/24	6	200
Vlan 7	10.239.70.2/24	7	200
Vlan 8	10.239.71.2/24	8	200
Gi0/23	10.239.128.2/24	23	200

Vlan	IP	Grupo	Prioridad
Vlan 2	10.239.65.3/24	2	100
Vlan 3	10.239.66.3/24	3	100
Vlan 4	10.239.67.3/24	4	100
Vlan 5	10.239.68.3/24	5	100
Vlan 6	10.239.69.3/24	6	100
Vlan 7	10.239.70.3/24	7	100
Vlan 8	10.239.71.3/24	8	100
Gi0/23	10.239.128.3/24	23	100

Vlan	IP	Grupo
Vlan 2	10.239.65.1/24	2
Vlan 3	10.239.66.1/24	3
Vlan 4	10.239.67.1/24	4
Vlan 5	10.239.68.1/24	5
Vlan 6	10.239.69.1/24	6
Vlan 7	10.239.70.1/24	7
Vlan 8	10.239.71.1/24	8
Gi0/23	10.239.128.1/24	23

Figura 3-52 Direccionamiento Switch capa núcleo del IATE



Vlan	IP	Grupo	Prioridad
Vlan 2	10.239.65.2/24	2	200
Vlan 3	10.239.66.2/24	3	200
Vlan 4	10.239.67.2/24	4	200
Vlan 5	10.239.68.2/24	5	200
Vlan 6	10.239.69.2/24	6	200
Vlan 7	10.239.70.2/24	7	200
Vlan 8	10.239.71.2/24	8	200
Gi0/23	10.239.128.2/24	23	200

Vlan	IP	Grupo	Prioridad
Vlan 2	10.239.65.3/24	2	100
Vlan 3	10.239.66.3/24	3	100
Vlan 4	10.239.67.3/24	4	100
Vlan 5	10.239.68.3/24	5	100
Vlan 6	10.239.69.3/24	6	100
Vlan 7	10.239.70.3/24	7	100
Vlan 8	10.239.71.3/24	8	100
Gi0/23	10.239.128.3/24	23	100

Figura 3-53 Interfaz Tracking para Switch Activo del IATE

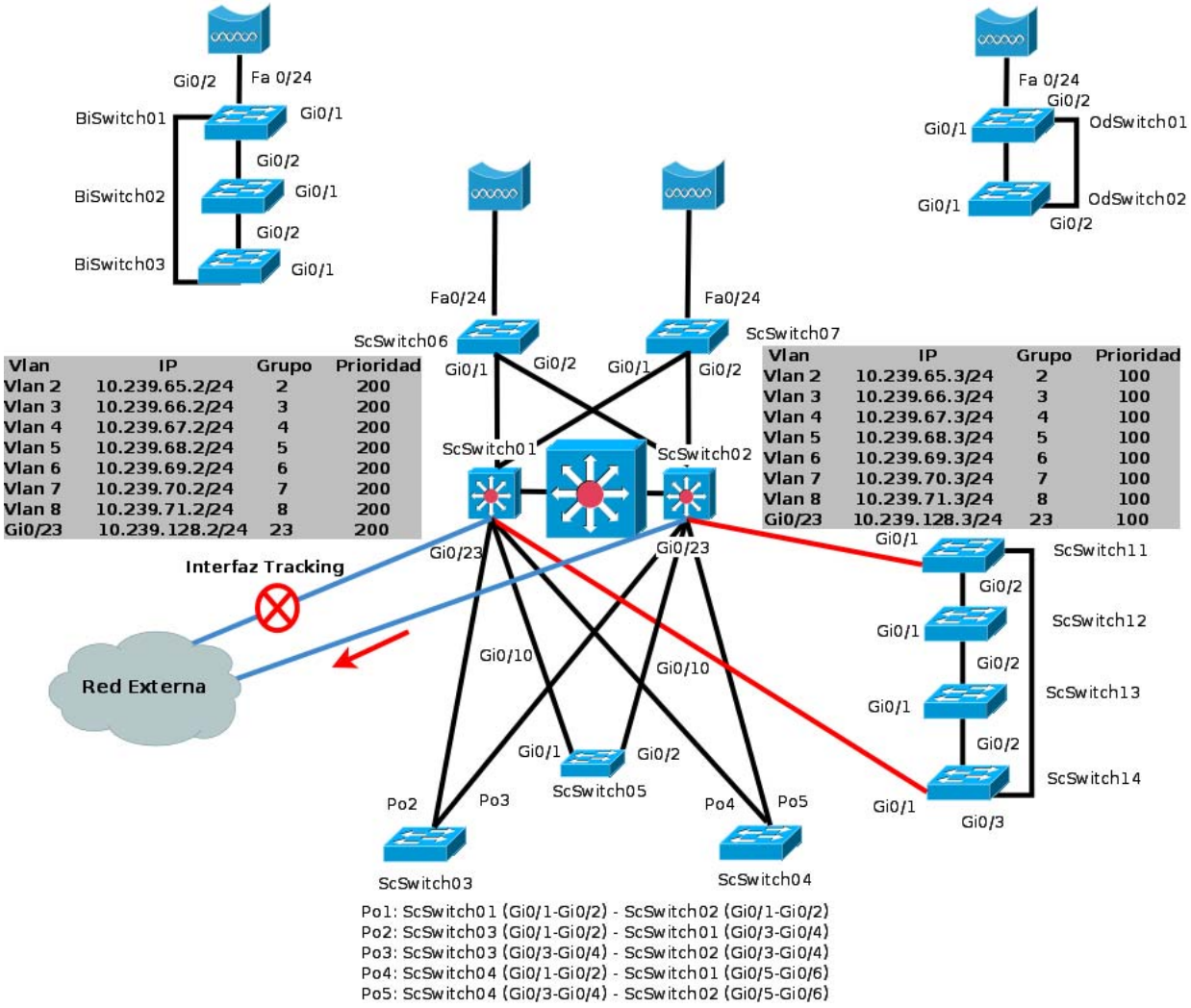


Figura 3-54 Caída Interfaz Tracking en Switch Activo

3.11 Conclusiones

Tras el trabajo realizado es posible afirmar que diseñar una red puede llegar a ser un gran desafío. Una red precisa de muchas características que la hagan fiable, manejable, fácil de gestionar y escalable, proporcionando conectividad usuario a usuario y usuario a aplicación, a una velocidad y fiabilidad razonable. Todo ello sin olvidar que el diseño debe ser adaptable, por lo que no debe incluir elementos que puedan limitar la implementación de nuevas tecnologías.

Teniendo en mente estas premisas, el proceso de diseño de la red del IATE se ha realizado aplicando el modelo de referencia jerárquico, resultando corresponderse con un modelo de núcleo colapsado. Al mismo tiempo se ha establecido como marco de trabajo el modelo de referencia OSI, clasificando los dispositivos requeridos según la capa en la que opera.

En esta sección también se ha presentado la arquitectura lógica y física de la red, analizando y justificando la elección de los elementos de comunicaciones tanto para la capa de acceso como para la capa distribución/núcleo, pertenecientes todos ellos a la familia Catalyst de Cisco, completísima línea de switches de alto rendimiento diseñados para ayudar a migrar de forma sencilla una red LAN compartida tradicional a una red completamente conmutada.

Por otra parte, como se apuntó en el capitulo anterior, uno de los grandes problemas en el IATE era la falta de documentación de red, por consiguiente, su elaboración ha supuesto una de las mayores aportaciones realizadas durante el desarrollo del presente proyecto. Documentar la red y mantener esta información actualizada de forma controlada, es un proceso laborioso y exige dotes de perseverancia, pero se considera un punto de partida ineludible y un paso previo a la implementación de cualquier mecanismo de seguridad.

Otro de los puntos extensamente tratado a lo largo del capítulo, ha sido la creación paso a paso de subredes virtuales, especialmente interesante en una empresa con distintos departamentos, ya que simplifican mucho el trabajo y la carga dentro de la red. Las VLANs además proporcionan seguridad, al segmentar servicios que potencialmente serían vulnerables frente a ataques.

Por ultimo, el capítulo finaliza tratando la redundancia a nivel de capa 2 y capa 3, así como los protocolos STP y HSRP, con el fin de mantener un alto grado de fiabilidad y evitar la inactividad de la red.

Sin embargo, como ya se apuntó en la introducción, el proceso de diseño de la red no finaliza en este punto, puesto que implica también abordar las decisiones de diseño relacionadas con la seguridad y la WLAN, cuestiones tratadas en los dos próximos capítulos.

Capítulo 4.
Seguridad

4.1 Introducción

Como ya se había adelantado con anterioridad, continuando con el proceso de diseño de la LAN, iniciado en el capítulo anterior, se hace imprescindible desarrollar una serie de puntos sobre las medidas de seguridad a aplicar.

El capítulo comienza introduciendo brevemente una serie de recomendaciones útiles para garantizar la seguridad básica de la red. Seguidamente se recogen las amenazas de seguridad a nivel de capa 2, así como las posibles medidas a adoptar con el fin de mitigarlas, y a continuación se trata la seguridad perimetral y el firewall. También incluye un apartado dedicado a las listas de control de acceso como medida de seguridad. Finalmente, la última sección del capítulo, presenta herramientas como NTop y ARPWatch, que facilitan la monitorización de la red.

4.2 Seguridad Básica

Para una mayor robustez y seguridad en la identificación y autenticación de usuarios es necesario seguir una serie de pautas que ayudarán a la elección de una buena contraseña.

El problema con las contraseñas es que cualquiera que sea útil es larga y difícil de recordar, por lo que el personal suele utilizar otras más sencillas. Las contraseñas no deben contener nombres de parientes o de mascotas, ni palabras que puedan encontrarse fácilmente en un diccionario. Tampoco deben sustituirse números por fonemas, o sustituir palabras por partes de palabras o sílabas, porque los hackers saben como localizar estas combinaciones.

Los ataques de diccionario, en los que las contraseñas se generan automáticamente, usando palabras comunes para obtener la combinación correcta, se han afinado para incluir estas combinaciones.

Para que una contraseña pueda considerarse como correcta no debe usar una secuencia de letras, debe tener al menos 8 caracteres de longitud y que estos pertenezcan a los cuatro conjuntos de

caracteres del teclado (mayúsculas, números, minúsculas y símbolos). Una buena contraseña contiene, al menos, un elemento de cada una de estas categorías.

Por desgracia, a los usuarios no suelen gustarle las contraseñas complejas. Esto suele desembocar en otro serio problema, ya que tienden a escribirlas en lugar de memorizarlas. Escribir una contraseña y dejarla cerca del PC es un gravísimo error de seguridad. Si fuera imprescindible almacenarla en el equipo ésta deberá permanecer cifrada. Por otra parte, las contraseñas deberían renovarse al menos cada 90 días.

Otra medida básica de seguridad con el fin de defender a los switches de capa 2 consiste en evitar el uso de Telnet, ya que es un protocolo inseguro. Si un atacante intercepta paquetes, podría ver en texto plano las credenciales de acceso al switch. Se recomienda siempre que sea posible sustituirlo por SSH (Secure Shell o shell segura),

SSH puede usarse en lugar de Telnet para conseguir una administración remota del router a través de conexiones que soportan privacidad estricta e integridad en la sesión. Esta conexión proporciona una funcionalidad que es similar a la de una conexión Telnet de salida excepto por el hecho de que está encriptada. Por tanto, SSH proporciona el mismo tipo de acceso que Telnet, con el beneficio agregado de seguridad, ya que la comunicación entre el cliente SSH y el servidor SSH está encriptada.

SSH pasó por algunas versiones en los dispositivos de Cisco, admitiendo actualmente SSHv1 y SSHv2. Cisco recomienda implementar SSHv2 cuando sea posible, debido a que utiliza un algoritmo de encriptación de seguridad mejor que SSHv1.

SSH admite el algoritmo estándar de encriptación de datos (DES, Data Encryption Standard), el algoritmo DES triple (3DES) y la autenticación de usuario basada en la contraseña. DES ofrece encriptación de 56 bits mientras que 3DES ofrece encriptación de 168 bits. La encriptación toma su tiempo, pero DES es más rápido que 3DES a la hora de encriptar texto.

Para implementar SSH se deben generar claves RSA. RSA incluye una clave pública, guardada en un servidor público de RSA y una clave privada, guardada sólo por el emisor y el receptor. La clave pública la pueden conocer todos y se utiliza para encriptar mensajes. Los mensajes encriptados con la clave pública sólo se pueden descifrar utilizando la clave privada.

4.3 Seguridad en capa 2

Los switches operan a nivel de capa 2. El modelo OSI está pensado para que cada capa opere independiente de las demás pero si un atacante gana el control de un switch, las capas superiores pueden ser comprometidas sin ser conscientes del problema, por lo que son un objetivo atractivo para los atacantes. En cuestión de seguridad en la red, la capa de enlace a menudo es la más débil.

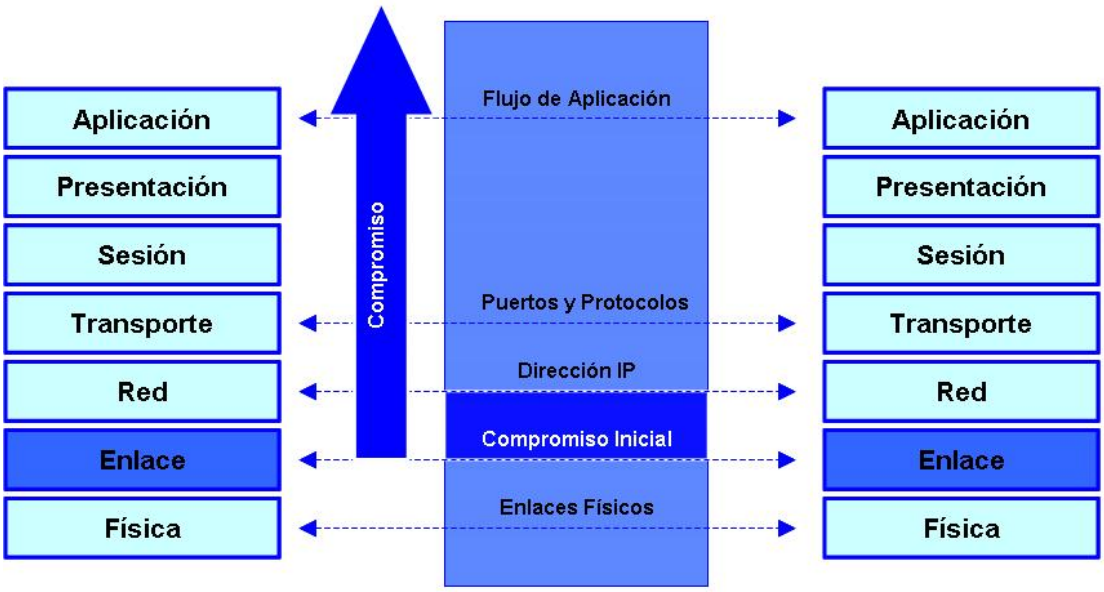


Figura 4-1 Seguridad en capa 2

Los ataques de capa 2 son lanzados desde dispositivos conectados a la red, ya sea sin autorización, una intrusión externa a un dispositivo autenticado, o bien tráfico originado desde un Host legítimo a la red. Las estadísticas demuestran que el 80% de los ataques provienen del interior de la organización.

En el presente proyecto fin de carrera, los ataques a nivel de capa 2 que se van a tratar se pueden clasificar según las siguientes categorías:

- Ataques de capa MAC
- Ataques VLAN
- Ataques por sustitución y/o simulación (spoofing)

4.3.1 Ataques MAC Flooding

La clave para entender cómo funcionan los ataques de desbordamiento MAC es conocer el tamaño limitado de las tablas Content-Addressable Memory (CAM), donde se especifica el puerto correspondiente a cada dirección MAC del switch, información que el switch posteriormente utilizará para tomar sus decisiones de envío. El switch tan solo enviará paquetes a través del puerto que conduzca a la máquina destino.

En la figura, el switch puede enviar tramas entre el PC1 y el PC2 sin inundar todos los puertos, puesto que la tabla de direcciones MAC mapea (puerto, dirección MAC) de estos PCs.

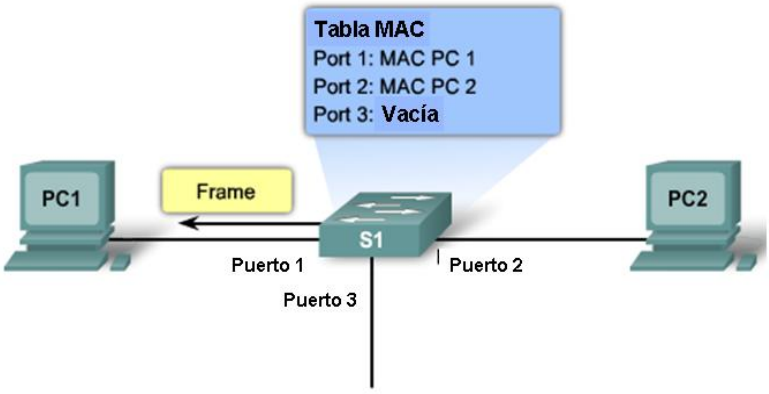


Figura 4-2 Ejemplo de estado correcto de la tabla MAC

El atacante se aprovecha de la limitación de las tablas CAM e inunda al switch, bombardeándolo con direcciones MAC falsas. Esto provoca que su tabla CAM se llene, hasta tal punto que las nuevas entradas no pueden ser aceptadas. Las consecuencias básicamente son dos:

- Lentitud en la red debido a que la CPU se pone al 70% - 80%
- Y en segundo lugar, que el switch acabe actuando como un simple concentrador, ya que comienza a retransmitir todo el tráfico que recibe a través de sus puertos, al no poder "recordar" qué equipos se encuentran conectados a sus distintas bocas o puertos. Como resultado, el atacante puede ver todos los paquetes enviados desde un host a otro dentro de la VLAN local a la que está conectado.

Si el ataque cesa, pasado un tiempo (habitualmente 4 horas de envejecimiento), el switch elimina las MAC aprendidas y empieza a funcionar correctamente.

La manera más común de llevar a cabo este tipo de ataque es mediante la herramienta macof, que se encarga de inundar al switch con frames que contienen las direcciones MAC e IP origen y destino. En un corto período de tiempo, la tabla de direcciones MAC se llena y entonces el

switch comienza a retransmitir a través de sus puertos todos los frames que recibe. Mientras la aplicación macof esté ejecutándose, el efecto seguirá siendo el mismo.

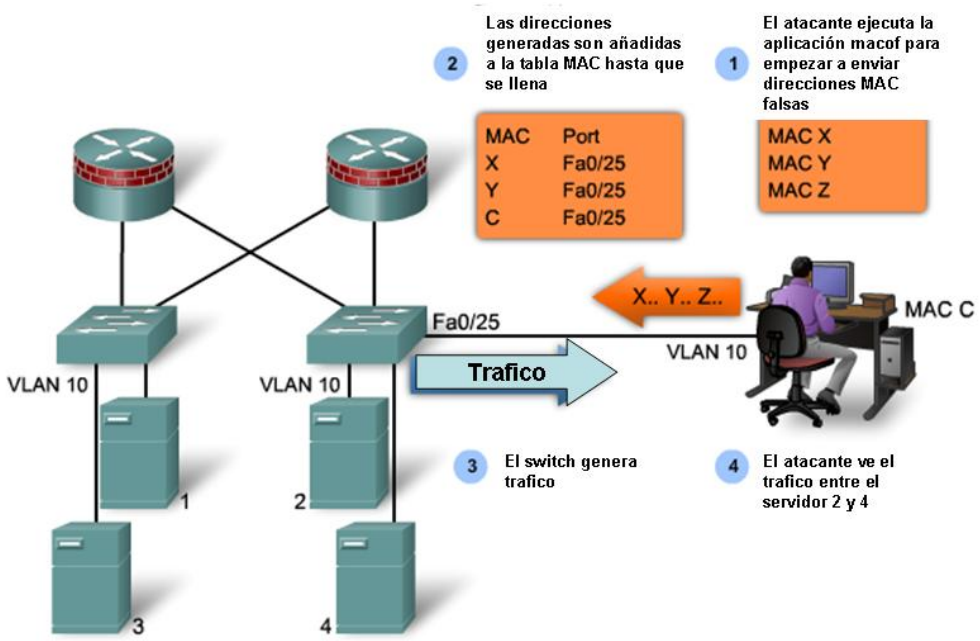


Figura 4-3 Ataque MAC Flooding

Los ataques MAC Flooding o también denominados CAM Table Overflow pueden evitarse mediante la configuración en el switch de seguridad en puerto. De este modo, el administrador puede especificar estáticamente las direcciones MAC de un puerto del switch en particular, o incluso permitir la opción de aprender dinámicamente un número fijo de direcciones MAC. En la Tabla 4-1 se resumen los distintos tipos de aprendizajes.

Afortunadamente, los switches Cisco incorporan seguridad en puerto (port security), característica que mitiga este efecto, identificando el número máximo de direcciones MAC permitidas por puerto.

Dirección MAC segura estática	▪ Se configura manualmente. ▪ Se agrega a la tabla de direcciones MAC. ▪ Se guarda en la running-configuration del switch ▪ Se puede hacer permanente guardando la configuración.
Dirección MAC segura dinámica	▪ Se aprende del tráfico que atraviesa la interfaz. ▪ Se guarda en la tabla de direcciones MAC. ▪ Se pierde cuando se reinicia el equipo.
Dirección MAC segura sticky	▪ Se puede configurar de forma manual o dinámica. ▪ Se guarda en la tabla de direcciones MAC. ▪ Se almacena en la running-configuration del switch. ▪ Se puede hacer permanente guardando la configuración.

Tabla 4-1 Port Security. Tipos de aprendizajes.

La principal ventaja de las direcciones sticky en contraposición con las dinámicas es que éstas últimas se agregan a la la running-configuration del switch. Así se evita escribir un montón de direcciones MAC de manera estática, pero además se pueden guardar en el archivo de configuración de manera que se mantengan inclusive si el switch se reinicia. Dos aspectos importantes a tener en cuenta:

- Si se habilitan las direcciones MAC sticky y ya había direcciones aprendidas de forma dinámica, éstas pasan a la running-configuration, y todas las nuevas que se aprendan también se agregan allí.

- Si se deshabilitan las direcciones MAC sticky, todas las que hubiera pasan a ser dinámicas y se borran de la running-configuration. Además, todas las que se aprendan también serán dinámicas.

Por violación se entiende que se ha alcanzado la cantidad máxima de direcciones MAC permitidas, o bien que una dirección MAC que se aprendió en un puerto se aprende por otro puerto diferente. Teniendo esto en cuenta, los modos en los que se puede establecer un puerto para decidir qué acción tomar en el caso de una violación son:

- **Protect**. Una vez que se alcanzó el máximo de direcciones MAC en un puerto, todo el tráfico de orígenes desconocidos (es decir, de direcciones MAC que no sean válidas para ese puerto) es descartado. No obstante, se continúa enviando el tráfico legal normalmente. No se notifica al administrador de esta situación.

- **Restrict.** El mismo comportamiento que el caso anterior pero con la diferencia que se envía un aviso al administrador mediante SNMP, se registra el evento en el syslog y se incrementa el contador de violaciones.

- **Shutdown.** En este caso, el puerto se da de baja dejándolo en estado err-disabled (deshabilitado por error). Además se envía un aviso al administrador mediante SNMP, se registra el evento en el syslog y se incrementa el contador de violaciones.

La Tabla 4-2 resume los principales puntos sobre el ataque MAC Flooding y las pruebas realizadas. Se puede observar que se han definido dos escenarios de pruebas, el primero de ellos, demuestra en la práctica que en una red no segura un atacante alcanza su objetivo, mientras el segundo de los escenarios, demuestra como llevando previamente a cabo las medidas necesarias se consigue mitigar el ataque.

Comenzando por el escenario de red no segura, se lanza el ataque. La Figura 4-5 refleja la hora en la que se iniciado, 17:34:25, y el número total de MACs disponibles en ese momento, 8091.

Por su parte, la Figura 4-6 muestra el proceso de inundación de las tablas CAM del switch. En la parte de la derecha de esta figura, aparecen las MACs generadas por el programa macof, y a la izquierda se demuestra que las MACs que están inundando la tabla son precisamente las generadas por dicho programa, como se puede observar, por ejemplo, en la línea resaltada en azul, correspondiente a la MAC 368a.8e35.7861 generada por macof.

Finalmente, la Figura 4-7 demuestra como el atacante consigue que la tabla CAM del switch se llene, ya que se puede apreciar que el número total de MACs disponible es 0. Este hecho ocurre a las 17:34:59, en tan solo 34 segundos después de haber iniciado el ataque, el atacante ha conseguido su objetivo.

La siguiente prueba consiste en repetir un proceso similar, tras previamente haber configurado en el dispositivo la seguridad en puerto. Se lanza el ataque mediante macof y como se puede ver en Figura 4-8 , una vez producida la violación del puerto, el switch deshabilita la boca y la pone en estado err-disable. Inmediatamente, como refleja la Figura 4-9 y Figura 4-10 , este suceso queda registrado en el servidor Syslog y en Nagios, quien además alerta al administrador de la red mediante un correo.

Ataque MAC Flooding				
Requerimiento:	➢ **REQ_07**: El administrador de red debe asegurar la integridad de la Content-Addressable Memory (CAM).			
Consecuencias de este ataque:	▪ Lentitud en la red debido a que la CPU se pone al 70% - 80% ▪ El switch actúa como simple concentrador, retransmitiendo el tráfico que recibe a través de sus puertos, al no poder "recordar" qué equipos se encuentran conectados a sus distintas bocas. De este modo, el atacante puede ver los paquetes enviados desde un host a otro dentro de la VLAN local a la que está conectado.			
Software utilizado:	macof			
Procedimiento para mitigar este ataque:	Se implementa port-security para limitar el número de MAC conectadas a un puerto. En caso de que se produzca una violación de puerto, la interfaz quedará en estado err-disable.			
Alarmas:	✓ Nagios ✓ Syslog			
Pasos			**Instrucciones**	**Referencias**
Escenario 1: Red No Segura	**1**	Lanzar ataque	Se lanza el programa macof	Figura 4-4 Ejecución de macof Figura 4-5 Total de MACs disponibles Figura 4-6 Tabla CAM del switch en proceso de inundación
	2	Resultado	Tabla CAM agotada	Figura 4-7 Tabla CAM inundada
Escenario 2: Red Segura	**1**	Medidas de mitigación	Configuración en el dispositivo de la seguridad en puerto.	Tratado en Capitulo 6. Seguridad en puerto
	2	Lanzar ataque	Se lanza el programa macof	Figura 4-4 Ejecución de macof
	3	Resultado	Violación de port security	Figura 4-8 Violación de port security Figura 4-9 Notificación del Syslog debido a violación de port security. Figura 4-10 Notificación del Nagios debido a violación de port security.

Tabla 4-2 Ataque MAC Flooding.

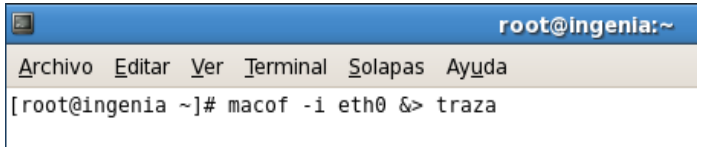


Figura 4-4 Ejecución de macof

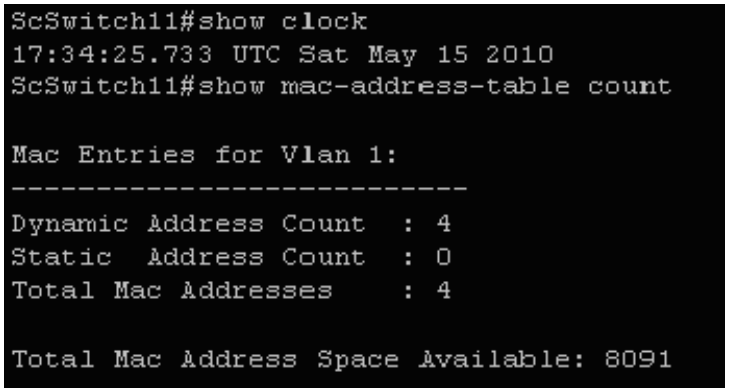
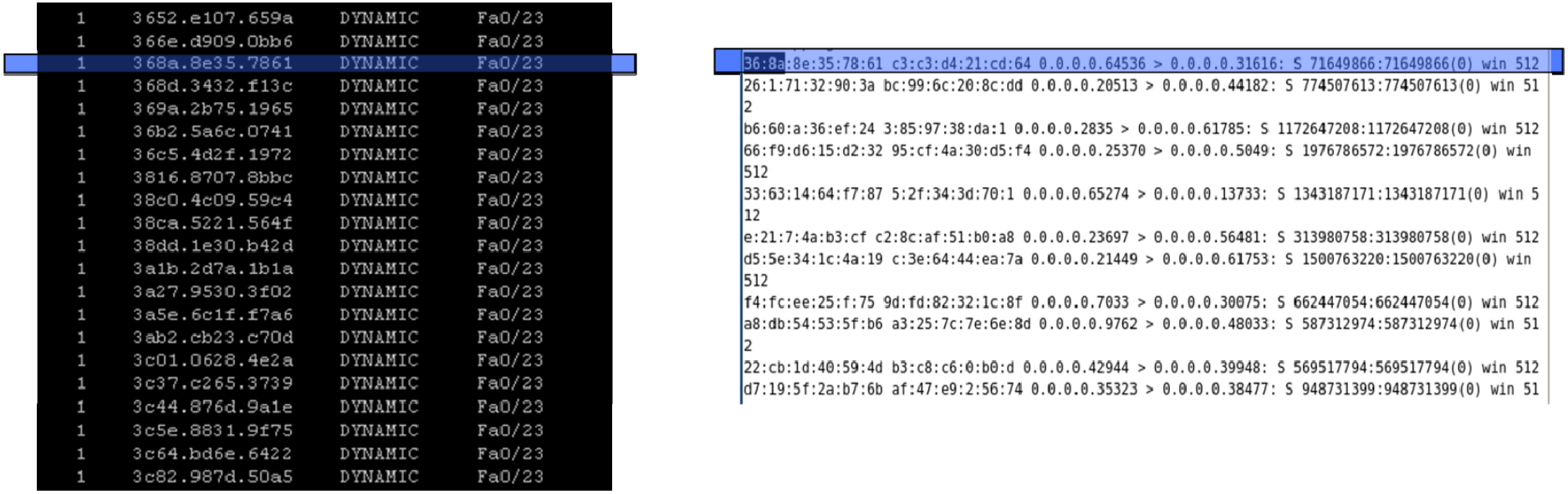


Figura 4-5 Total de MACs disponibles



1	3652.e107.659a	DYNAMIC	Fa0/23
1	366e.d909.0bb6	DYNAMIC	Fa0/23
1	368a.8e35.7861	DYNAMIC	Fa0/23
1	368d.3432.f13c	DYNAMIC	Fa0/23
1	369a.2b75.1965	DYNAMIC	Fa0/23
1	36b2.5a6c.0741	DYNAMIC	Fa0/23
1	36c5.4d2f.1972	DYNAMIC	Fa0/23
1	3816.8707.8bbc	DYNAMIC	Fa0/23
1	38c0.4c09.59c4	DYNAMIC	Fa0/23
1	38ca.5221.564f	DYNAMIC	Fa0/23
1	38dd.1e30.b42d	DYNAMIC	Fa0/23
1	3a1b.2d7a.1b1a	DYNAMIC	Fa0/23
1	3a27.9530.3f02	DYNAMIC	Fa0/23
1	3a5e.6c1f.f7a6	DYNAMIC	Fa0/23
1	3ab2.cb23.c70d	DYNAMIC	Fa0/23
1	3c01.0628.4e2a	DYNAMIC	Fa0/23
1	3c37.c265.3739	DYNAMIC	Fa0/23
1	3c44.876d.9a1e	DYNAMIC	Fa0/23
1	3c5e.8831.9f75	DYNAMIC	Fa0/23
1	3c64.bd6e.6422	DYNAMIC	Fa0/23
1	3c82.987d.50a5	DYNAMIC	Fa0/23

```
36:8a:8e:35:78:61 c3:c3:d4:21:cd:64 0.0.0.0.64536 > 0.0.0.0.31616: S 71649866:71649866(0) win 512
26:1:71:32:90:3a bc:99:6c:20:8c:dd 0.0.0.0.20513 > 0.0.0.0.44182: S 774507613:774507613(0) win 51
2
b6:60:a:36:ef:24 3:85:97:38:da:1 0.0.0.0.2835 > 0.0.0.0.61785: S 1172647208:1172647208(0) win 512
66:f9:d6:15:d2:32 95:cf:4a:30:d5:f4 0.0.0.0.25370 > 0.0.0.0.5049: S 1976786572:1976786572(0) win
512
33:63:14:64:f7:87 5:2f:34:3d:70:1 0.0.0.0.65274 > 0.0.0.0.13733: S 1343187171:1343187171(0) win 5
12
e:21:7:4a:b3:cf c2:8c:af:51:b0:a8 0.0.0.0.23697 > 0.0.0.0.56481: S 313980758:313980758(0) win 512
d5:5e:34:1c:4a:19 c:3e:64:44:ea:7a 0.0.0.0.21449 > 0.0.0.0.61753: S 1500763220:1500763220(0) win
512
f4:fc:ee:25:f:75 9d:fd:82:32:1c:8f 0.0.0.0.7033 > 0.0.0.0.30075: S 662447054:662447054(0) win 512
a8:db:54:53:5f:b6 a3:25:7c:7e:6e:8d 0.0.0.0.9762 > 0.0.0.0.48033: S 587312974:587312974(0) win 51
2
22:cb:1d:40:59:4d b3:c8:c6:0:b0:d 0.0.0.0.42944 > 0.0.0.0.39948: S 569517794:569517794(0) win 512
d7:19:5f:2a:b7:6b af:47:e9:2:56:74 0.0.0.0.35323 > 0.0.0.0.38477: S 948731399:948731399(0) win 51
```

Figura 4-6 Tabla CAM del switch en proceso de inundación

```
ScSwitch11#show mac-address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count   : 8088
Static  Address Count   : 0
Total Mac Addresses     : 8088

Total Mac Address Space Available: 0

ScSwitch11#show clock
17:34:59.220 UTC Sat May 15 2010
ScSwitch11#
```

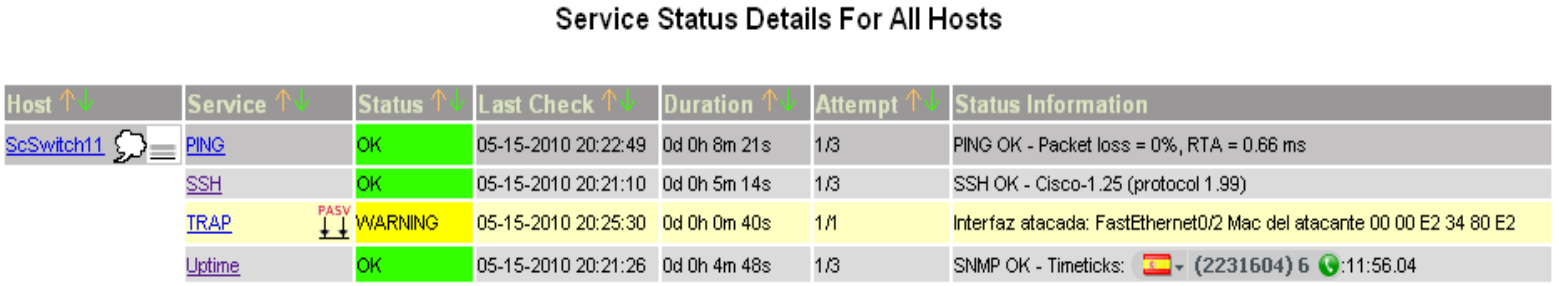
Figura 4-7 Tabla CAM inundada

```
ScSwitch11#
000045: .May 15 18:11:30: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/23, putting Fa0/23 in err-disable state
000046: .May 15 18:11:30: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address a822.c94b.9440 on port FastEthernet0/23.
000047: .May 15 18:11:31: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to down
000048: .May 15 18:11:32: %LINK-3-UPDOWN: Interface FastEthernet0/23, changed state to down
ScSwitch11#
ScSwitch11#
```

Figura 4-8 Violación de port security

```
[root@ingenia ~]# tail -f /var/log/cisco/cisco.log
May 15 20:23:01 192.168.1.254 56: 000054: May 15 18:22:59: %SYS-5-CONFIG_I: Configured from console by console
May 15 20:23:02 192.168.1.254 57: 000055: May 15 18:23:01: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/2, putting Fa0/2 in err-disable state
May 15 20:23:03 192.168.1.254 58: 000056: May 15 18:23:01: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0000.e234.80e2 on port FastEthernet0/2.
May 15 20:25:23 192.168.1.254 59: 000057: May 15 18:25:20: %SYS-5-CONFIG_I: Configured from console by console
May 15 20:25:26 192.168.1.254 60: 000058: May 15 18:25:23: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
May 15 20:25:26 192.168.1.254 61: 000059: May 15 18:25:24: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
May 15 20:25:27 192.168.1.254 62: 000060: May 15 18:25:26: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/2, putting Fa0/2 in err-disable state
May 15 20:25:28 192.168.1.254 63: 000061: May 15 18:25:26: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0000.e234.80e2 on port FastEthernet0/2.
May 15 20:25:28 192.168.1.254 64: 000062: May 15 18:25:27: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
May 15 20:25:30 192.168.1.254 65: 000063: May 15 18:25:28: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down
```

Figura 4-9 Notificación del Syslog debido a violación de port security.



Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
ScSwitch11	PING	OK	05-15-2010 20:22:49	0d 0h 8m 21s	1/3	PING OK - Packet loss = 0%, RTA = 0.66 ms
	SSH	OK	05-15-2010 20:21:10	0d 0h 5m 14s	1/3	SSH OK - Cisco-1.25 (protocol 1.99)
	TRAP PASV	WARNING	05-15-2010 20:25:30	0d 0h 0m 40s	1/1	Interfaz atacada: FastEthernet0/2 Mac del atacante 00 00 E2 34 80 E2
	Uptime	OK	05-15-2010 20:21:26	0d 0h 4m 48s	1/3	SNMP OK - Timeticks: (2231604) 6 :11:56.04

"***** Nagios *****

Notification Type: PROBLEM

Service: TRAP

Host: ScSwitch11

Address: 192.168.1.254

State: WARNING

Date/Time: Sat May 15 20:26:07 CEST 2010

Additional Info: Interfaz atacada: FastEthernet0/2 Mac del atacante 00 00 E2 34 80 E2"

Figura 4-10 Notificación del Nagios debido a violación de port security.

4.3.2 Ataques VLAN

Este apartado está enfocado al ataque conocido como VLAN Hopping, que permite pasar tráfico de una VLAN a otra sin que haya sido enrutado previamente.

Las VLANs se implementan para generar un control de tráfico entre las mismas, de forma que los equipos conectados a una VLAN no posean acceso a otras. Pues precisamente este tipo de ataque pretende engañar a un switch, sobre el cual se implementan VLANs, mediante técnicas que logran conocer los paquetes de información que circulan entre ellas, y como consecuencia alcanzar un host de otra VLAN distinta a la del atacante. Los dos enfoques para ejecutar este tipo de ataque son Switch Spoofing y Doble Etiquetado (double tagging).

Antes de continuar, un inciso para recordar que los puertos trunk por defecto tienen acceso a todas las VLANs. Se emplean para transmitir tráfico de múltiples VLANs a través del mismo enlace físico (generalmente empleado para conectar switches). La encapsulación puede ser IEEE 802.1Q o ISL.

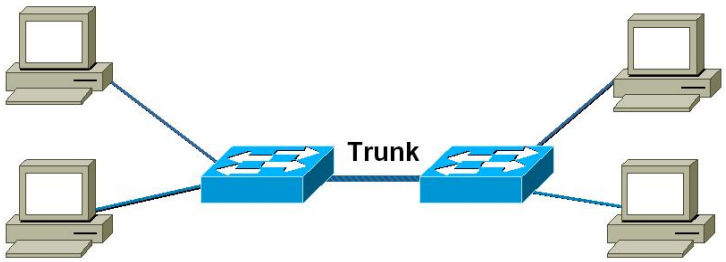


Figura 4-11 Dynamic Trunking Protocol (DTP)

El Dynamic Trunking Protocol (DTP) es un protocolo propietario que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLANs con ISL o 802.1Q) en enlaces Ethernet, con objeto de hacer innecesaria la intervención administrativa en los extremos. Dicho protocolo puede establecer los puertos Ethernet en cinco modos diferentes de trabajo: AUTO, ON, OFF, DESIRABLE y NON-NEGOTIATE. Por defecto, en la mayoría de los switches se establece a modo auto.

4.3.2.1 Switch Spoofing

Se deduce de lo anterior que por defecto, los enlaces troncales de los switches Ethernet portan tráfico de todas las VLAN. El ataque Switch Spoofing consiste en hacerse pasar por un switch,

intentando conectarse a un puerto del mismo y forzándolo a trabajar en modo trunk para tener acceso a todas las VLANs. El efecto es que el equipo se vuelve miembro de todas las VLAN.

Figura 4-12 Ataque Switch Spoofing

Esta amenaza se suele usar con el fin de descubrir las credenciales de autenticación de los usuarios de la red. La forma de llevarla a cabo es mediante un software especial que permita al PC actuar como una especie de switch virtual, que usaría DTP para negociar un trunk, y de esa manera conseguir capturar el tráfico de todas las VLAN.

Para mitigar esta amenaza se pueden configurar los puertos del switch en modo acceso.

La Tabla 4-3 resume los principales puntos sobre el ataque Switch Spoofing y las pruebas realizadas. Se puede observar que también se han definido dos escenarios de pruebas, el primero de ellos, demuestra en la práctica que en una red no segura un atacante alcanza su objetivo, mientras el segundo de los escenarios, demuestra como llevando previamente a cabo las medidas necesarias se consigue mitigar el ataque.

Comenzando por el escenario de red no segura, se lanza el ataque. En la Figura 4-13 se puede ver como el software Yersina permite llevar a cabo un ataque DTP. Tras esto, la Figura 4-14 , demuestra como el atacante consigue establecer un TRUNK/DESIRABLE, y efectivamente, la Figura 4-15 muestra que la interfaz Fa0/12 del switch está en modo TRUNK.

La siguiente prueba consiste en repetir un proceso similar, tras previamente haber deshabilitado DTP al establecer la interfaz en modo acceso, como refleja la Figura 4-16 . De nuevo se lanza el ataque con Yersina y como se puede ver en la Figura 4-17 , una vez que la interfaz está en modo acceso, el atacante no consigue establecer un Trunk

Ataque Switch Spoofing				
Requerimiento:			➢ **REQ_08**: El administrador de red debe asegurar que ningún puerto del switch va a negociar un Trunk usando DTP	
Consecuencias de este ataque:			El atacante consigue crear un Trunk, pudiendo de esta manera ver todo el tráfico que pasa por la red.	
Software utilizado:			Yersinia	
Procedimiento para mitigar este ataque:			Configurar los puertos del switch en modo acceso. Esto provocará que se deshabilite DTP en todos los puertos que no necesiten formar un enlace troncal.	
Alarmas:			-----	
Pasos			**Instrucciones**	**Referencias**
Escenario 1: Red No Segura	**1**	Lanzar ataque	Se lanza el ataque mediante el software Yersinia.	Figura 4-13 Selección del ataque DTP
	2	Resultado	El atacante consigue establecer un Trunk con el switch	Figura 4-14 Establecimiento de un Trunk Figura 4-15 Interfaces Trunk en el switch
Escenario 2: Red Segura	**1**	Medidas de mitigación 1	Configuración de los puertos del switch. Determinar que puertos van a estar en modo acceso y cuales en modo Trunk.	Tratado en Capitulo 6. Configuración de puertos Figura 4-16 Desactivación de DTP
	2	Lanzar ataque	Se lanza el ataque mediante el software Yersinia.	Figura 4-13 Selección del ataque DTP
	3	Resultado	El atacante no consigue establecer un Trunk con el switch	Figura 4-17 No se consigue establecer un Trunk

Tabla 4-3 Ataque Switch Spoofing.

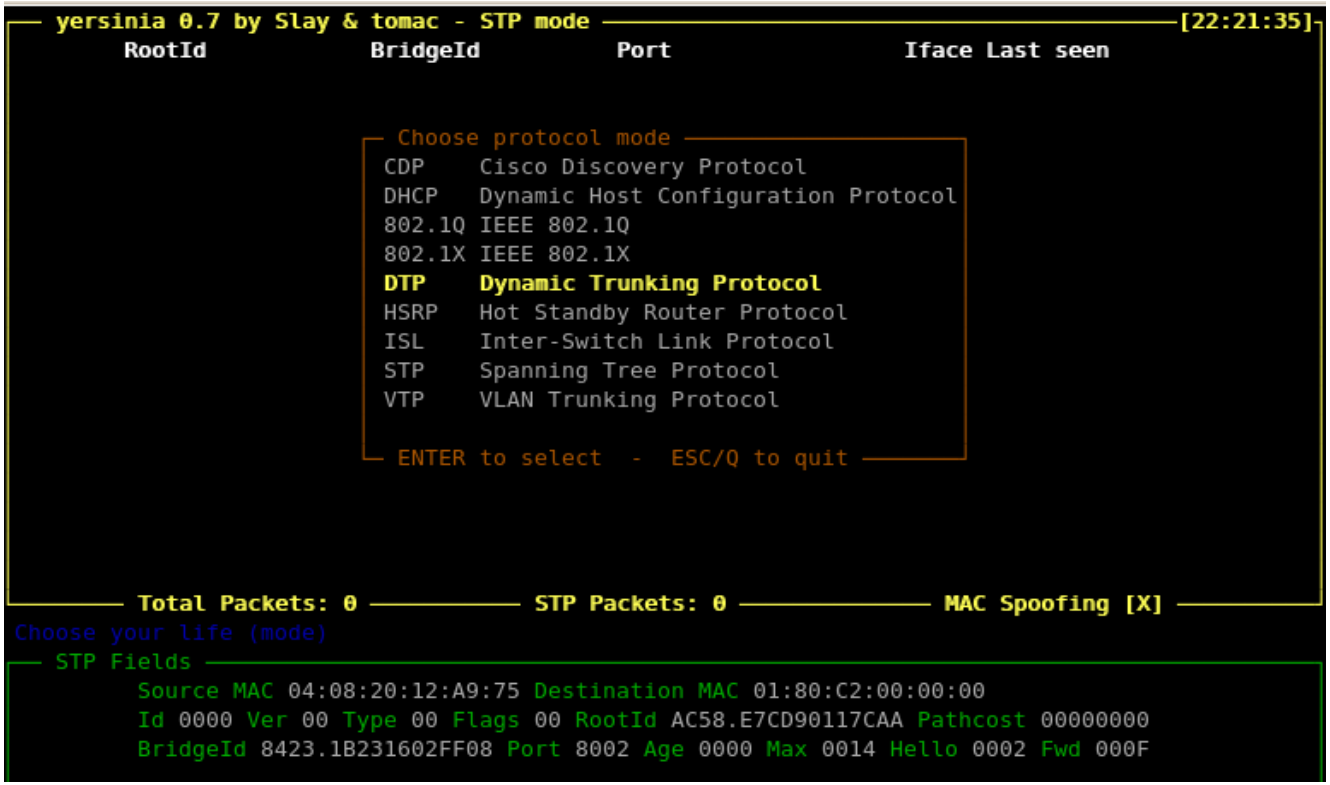


Figura 4-13 Selección del ataque DTP

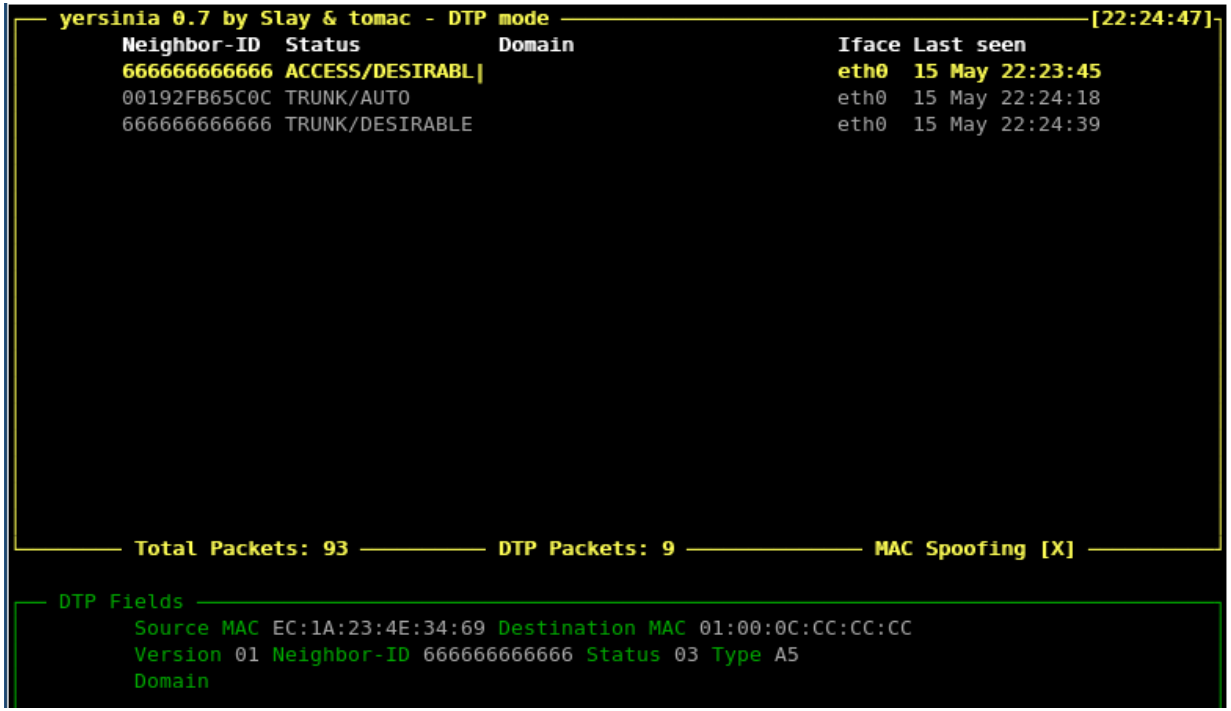


Figura 4-14 Establecimiento de un Trunk

```
ScSwitch11#show interfaces tru
ScSwitch11#show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/12      auto         802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/12      1-4094

Port        Vlans allowed and active in management domain
Fa0/12      1-2

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/12      1-2
ScSwitch11#
```

Figura 4-15 Interfaces Trunk en el switch

```
ScSwitch11(config)#interface fastEthernet 0/12
ScSwitch11(config-if)#switchport mode access
```

Figura 4-16 Desactivación de DTP

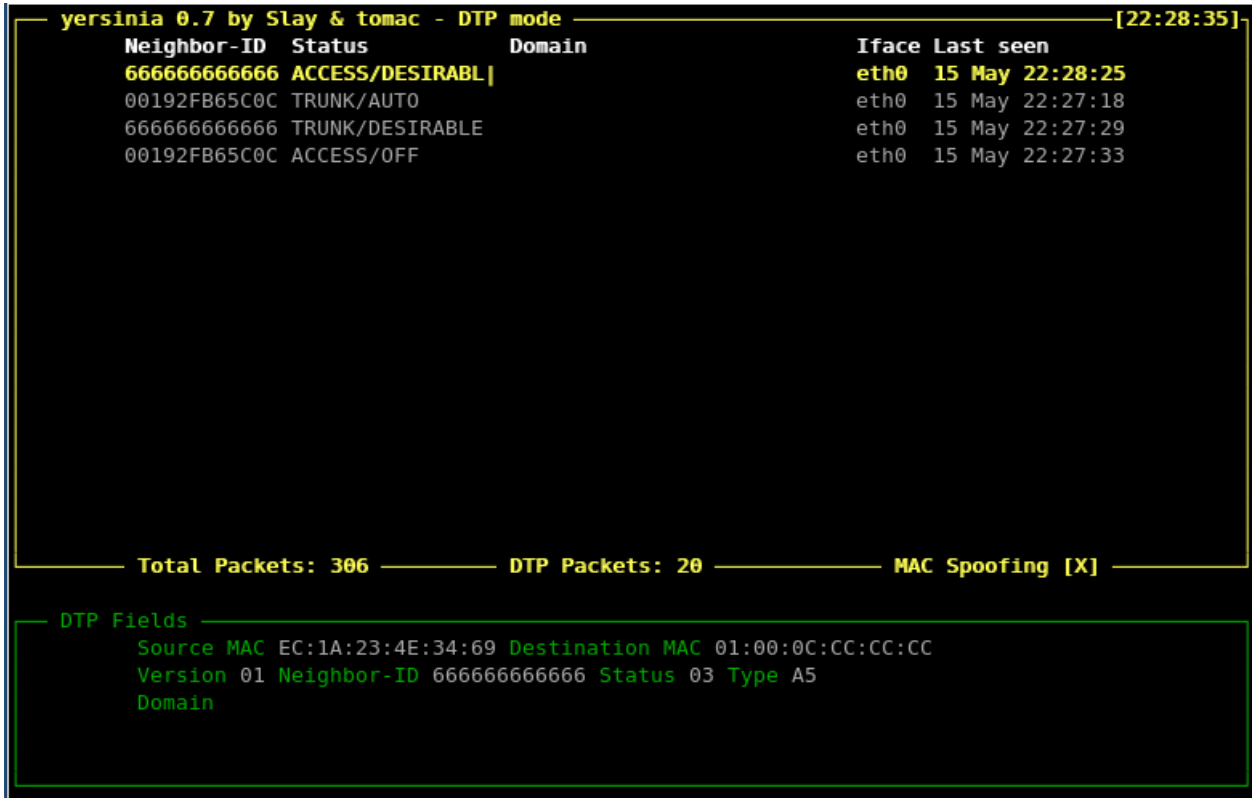


Figura 4-17 No se consigue establecer un Trunk

4.3.2.2 Doble Etiquetado

En un enlace troncal, una VLAN es designada como la nativa. Esta VLAN no añade ningún etiquetado a sus tramas pero sí etiqueta las tramas de las demás VLANs. Si un PC de usuario pertenece a la VLAN nativa, el atacante puede aprovecharse de esta situación.

Este ataque es unidireccional (no recibe respuesta) y sólo puede utilizarse si el atacante se encuentra en la misma VLAN nativa que el puerto trunk, sin embargo, funciona aunque el puerto del atacante tenga el estado de trunking off.

Su filosofía consiste en etiquetar dos veces una trama, primero con la etiqueta de la VLAN destino y después con la de la VLAN nativa. El atacante envía esta trama al primer switch y éste al ver que se dirige a la VLAN nativa, elimina su etiqueta e inunda la trama por todos los puertos de la VLAN nativa (en el caso que desconozca el destinatario), incluyendo a través del enlace troncal, y conservando el etiquetado de la VLAN destino que insertó el atacante. Cuando llega al segundo switch, éste observa que se dirige a la VLAN de destino e inunda la trama por todos los puertos de la VLAN destino (en el caso que desconozca el destinatario), consiguiendo con esto alcanzar una VLAN distinta sin pasar por un dispositivo de Capa 3.

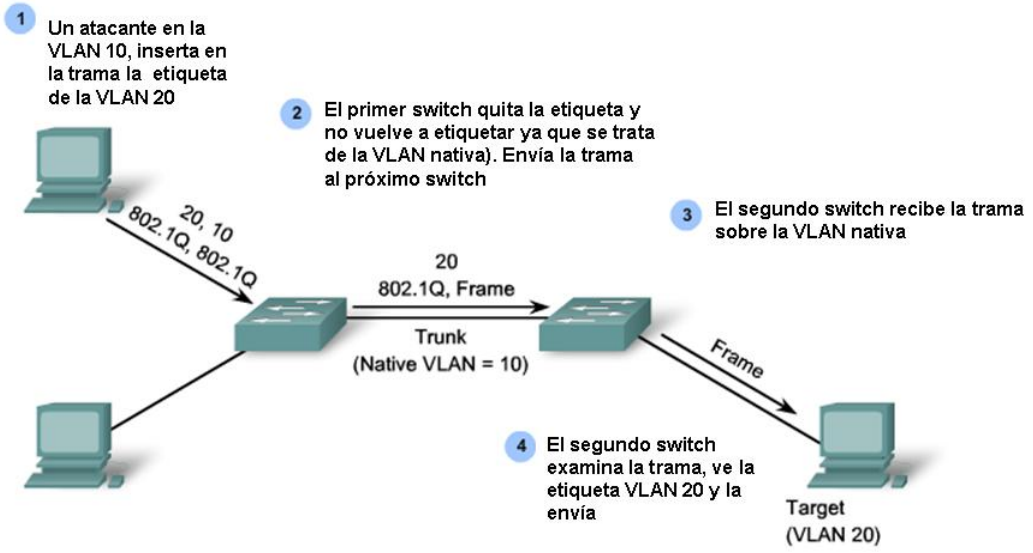


Figura 4-18 Ataque Doble Etiquetado

Para llevar a cabo este tipo de ataque es necesario el uso de programas tales como Yersinia, que permite enviar tramas desde un host con una etiqueta de VLAN insertada.

En este sentido, algunas prácticas recomendadas para mitigar esta amenaza son utilizar VLANs diferentes a la nativa para enviar el tráfico de usuario y añadir todos los puertos no utilizados a una VLAN sin uso. Por su parte, la Tabla 4-4 resume los pasos seguidos con el fin de mitigar este ataque.

Ataque Doble Etiquetado				
Requerimiento:			➢ **REQ_09**: El administrador de red debe asegurar que ningún usuario pertenece a la VLAN nativa.	
Consecuencias de este ataque:			El atacante etiqueta dos veces una trama, primero con la etiqueta de la VLAN destino y después con la etiqueta de la VLAN nativa. Esto permite que se pueda alcanzar una VLAN distinta sin pasar por un dispositivo de Capa 3.	
Software utilizado:			-----	
Procedimiento para mitigar este ataque:			Utilizar VLAN diferentes a la nativa para enviar tráfico de usuario.	
Alarmas:			-----	
Pasos			**Instrucciones**	**Referencias**
Escenario: Red Segura	**1**	Medida de mitigación 1	Deshabilitar la VLAN nativa, que por defecto es la VLAN1.	Tratado en Capitulo 6. Configuración de puertos
	2	Medida de mitigación 2	Configurar cada puerto del switch en su VLAN correspondiente. Si el puerto no está operativo deshabilitarlo.	Tratado en Capitulo 6. Configuración de puertos

Tabla 4-4 Ataque Doble Etiquetado

4.3.3 Ataques por sustitución y/o simulación (Spoofing)

Los ataques de spoofing ocurren cuando el atacante se hace pasar por otro para eludir las configuraciones de seguridad, recibir los datos destinado a un equipo objetivo, manipular el tráfico local o incluso detenerlo, conocido como DoS (Denegación de Servicio). En este sentido, en el presente proyecto se van a tratar los siguientes ataques:

- DHCP Spoofing
- MAC Spoofing
- ARP Spoofing
- Ataques STP

4.3.3.1 DHCP Spoofing

En la mayoría de las redes actuales los clientes obtienen su dirección IP de forma dinámica, usando DHCP, de tal modo que para obtener su información de direccionamiento, el cliente envía una petición DHCP a la que el servidor responde.

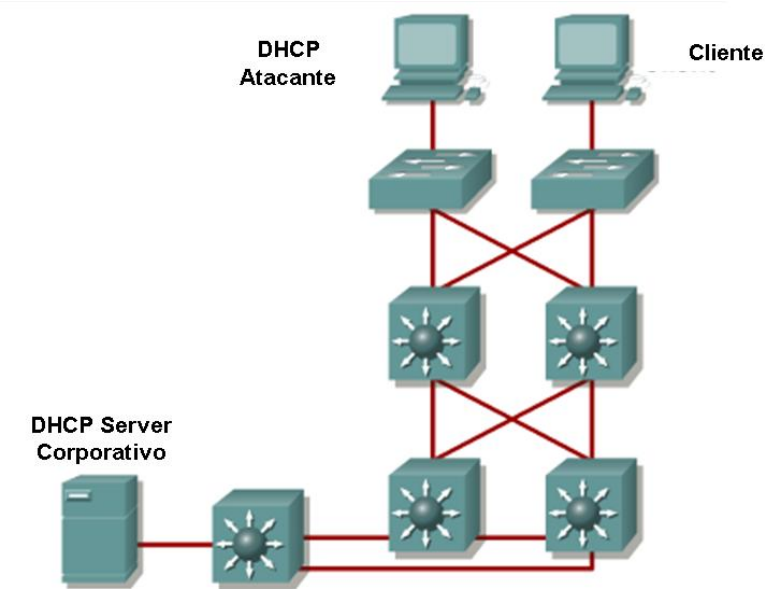


Figura 4-19 Ataque DHCP Spoofing

Uno de los modos en los que un atacante puede tener acceso al tráfico de la red es mediante un dispositivo DHCP infiltrado en la red, que responda a las consultas de los clientes DHCP, indicándole su propia IP como puerta de enlace o servidor DNS (Domain Name System), y por

consiguiente “envenenando” tales respuestas. Si bien es cierto que el servidor legítimo también puede responder, si el dispositivo spoofing está en el mismo segmento que el cliente, su respuesta puede llegarle primero. De este modo, el cliente estaría enviando el tráfico a la dirección IP del atacante en lugar de hacerlo al router correspondiente. Desde la perspectiva del cliente todo funciona correctamente. Esta amenaza también conocida como ataque “man-in-the-middle” es difícil de detectar.

Otra estrategia es el ataque DHCP DoS (Denegación de Servicio DHCP), que consiste en agotar el pool de direcciones que un servidor DHCP puede proporcionar a los clientes, pidiéndole de forma reiterada direcciones IP. Para ello el atacante manda cada solicitud DHCP con una MAC falsificada, de tal forma que el servidor lo interpreta como una solicitud cualquiera.

La solución para combatir los ataques tanto por “envenenamiento” como por “agotamiento” es la característica DHCP Snooping de los switches Cisco, que permite especificar qué puertos puede contestar a solicitudes DHCP. Los puertos que se configuren como seguros podrán contestar y enviar solicitudes DHCP, mientras que los puertos inseguros solo podrán enviar peticiones.

De este modo, la práctica recomendable es configurar como puertos seguros (trusted port) aquellos que contengan servidores legítimos y como inseguros (untrusted port) los puertos de usuario. En el momento en el que un puerto inseguro reciba una respuesta (DHCPOFFER, DHCPACK, DHCPNAK) a una solicitud DHCP, quedaría deshabilitado automáticamente.

No es necesario configurar todos los puertos del switch para soportar DHCP snooping. Si un puerto no es configurado de forma explícita como seguro, de forma implícita es considerado un puerto inseguro.

Por otra parte, la prestación “DHCP Snooping” también sirve para limitar el número de mensajes DHCP por segundo permitidos en una interfaz.

La siguiente figura muestra que puertos se van a configurar como seguros en la red del IATE. Estos serán, por tanto, desde los que se permitirá recibir y enviar peticiones DHCP. El resto de puertos será considerado inseguro.

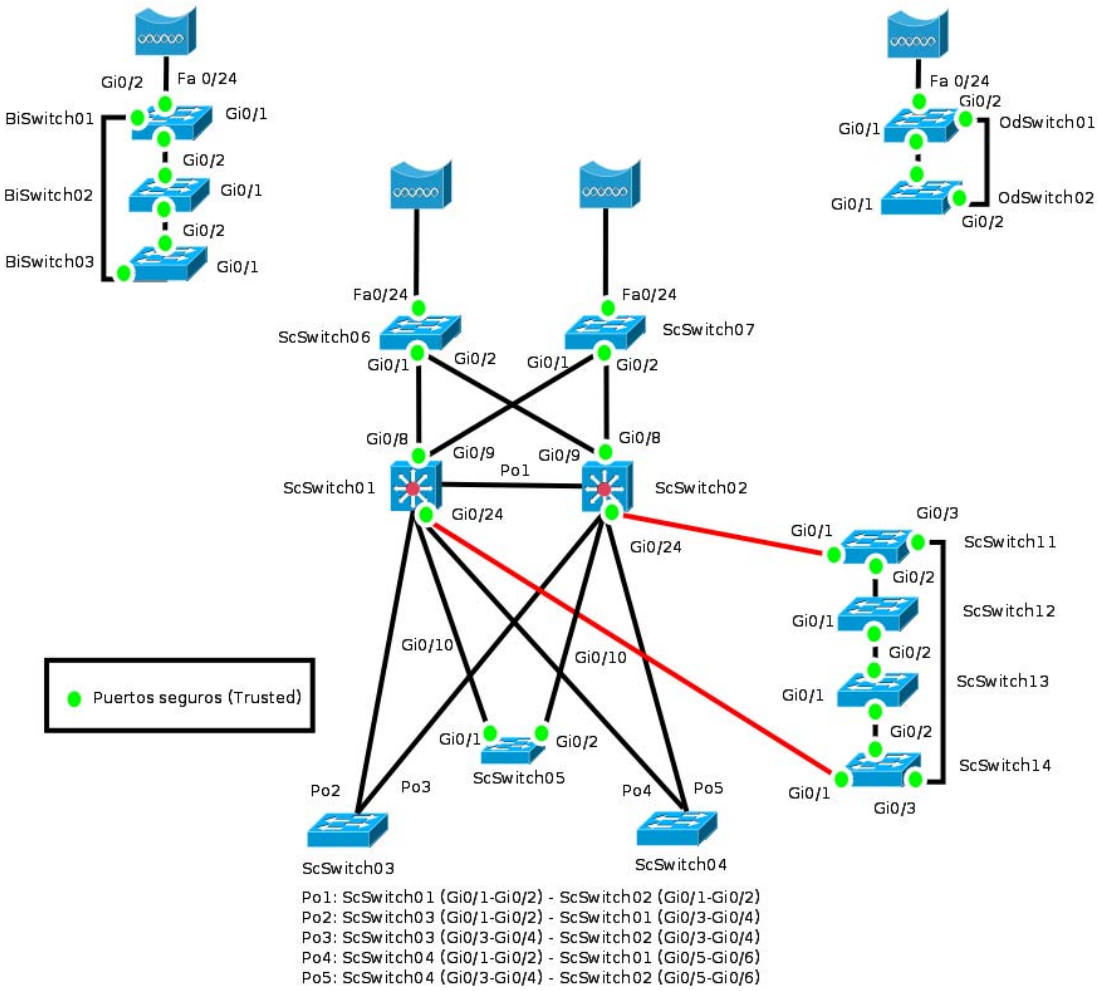


Figura 4-20 DHCP Spoofing. Puertos seguros (Trusted)

La Tabla 4-5 resume los principales puntos sobre el ataque DHCP Spoofing y las pruebas realizadas. Se puede observar que se han definido dos escenarios de pruebas, el primero de ellos, demuestra en la práctica que en una red no segura un atacante alcanza su objetivo, mientras el segundo de los escenarios, demuestra como llevando previamente a cabo las medidas necesarias se consigue mitigar el ataque.

Comenzando por el escenario de red no segura, se lanza el ataque. La Figura 4-21 presenta los diferentes tipos de ataques DHCP que permite ejecutar Yersina. En esta prueba, se lanza el ataque 1 (Sending Discovery Packet), como se aprecia en la Figura 4-22. Como consecuencia, el atacante consigue la denegación del servicio, como se demuestra en la Figura 4-23.

La siguiente prueba consiste en repetir un proceso similar, tras previamente haber configurado DHCP Snooping y limitar el número de peticiones de DHCP por puerto a 15. De nuevo se lanza el ataque con Yersina y como se puede ver en la Figura 4-24, en el momento que la interfaz recibe más de 15 peticiones de solicitud DHCP, la interfaz Fa0/24 del switch queda deshabilitada automáticamente, bloqueando el ataque DHCP.

Ataque DHCP Spoofing				
Requerimiento:			➢ **REQ_10**: El administrador debe asegurar que no se instalan DHCP no legítimos y evitar ataques de DoS sobre el servidor DHCP	
Consecuencias de este ataque:			▪ En los ataques "hombre en el medio", el dispositivo DHCP infiltrado puede actuar como servidor DHCP, respondiendo a consultas de los clientes DHCP con su propia IP como puerta de enlace o servidor DNS. De este modo, el atacante consigue recibir el tráfico enviado por el cliente. ▪ En los ataques DHCP DoS, se agota el pool de direcciones que un servidor DHCP puede proporcionar a sus clientes. De este modo, el atacante consigue la denegación del servicio.	
Software utilizado:			Yersinia	
Procedimiento para mitigar este ataque:			▪ La característica DHCP Snooping de Cisco permite especificar que puertos puede contestar a solicitudes DHCP. Los puertos seguros podrán contestar y enviar solicitudes DHCP, mientras que los inseguros solo podrán enviar peticiones. La práctica recomendada es configurar como puertos seguros aquellos que contengan servidores legítimos y como inseguros los de usuario. Cuando un puerto inseguro recibe una respuesta a una solicitud DHCP, queda deshabilitado automáticamente. ▪ Para mitigar los ataques DHCP DoS es posible limitar el número de peticiones DHCP por interfaz.	
Alarmas:			-----	
Pasos			**Instrucciones**	**Referencias**
Escenario 1: Red No Segura	**1**	Lanzar ataque	Se lanza el ataque mediante el software Yersinia	Figura 4-21 Yersina. Tipos de ataques DHCP Figura 4-22 Ejecución del ataque 1. Enviando Discovery Packet
	2	Resultado	Denegación del servicio en el switch de capa 3, que en el IATE es el correspondiente al servidor DHCP.	Figura 4-23 Denegación del servicio
Escenario 2: Red Segura	**1**	Medidas de mitigación	Configurar DHCP Snooping y limitar el número de peticiones de DHCP por puerto a 15.	Tratado en Capitulo 6. Configuración DHCP Snooping
	2	Lanzar ataque	Se lanza el ataque mediante el software Yersinia	Figura 4-21 Yersina. Tipos de ataques DHCP
	3	Resultado	La interfaz del switch se pone en modo err-disable.	Figura 4-24 Bloqueo del ataque DHCP

Tabla 4-5 Ataque DHCP Spoofing.

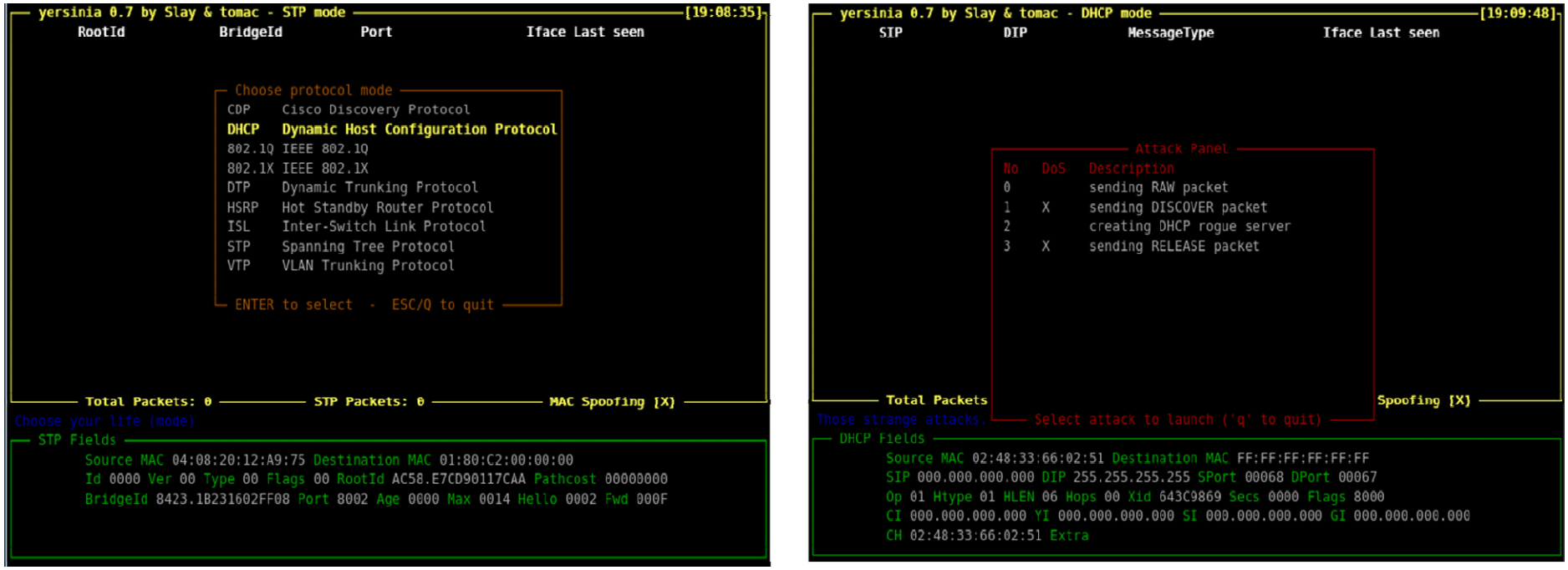


Figura 4-21 Yersina. Tipos de ataques DHCP.

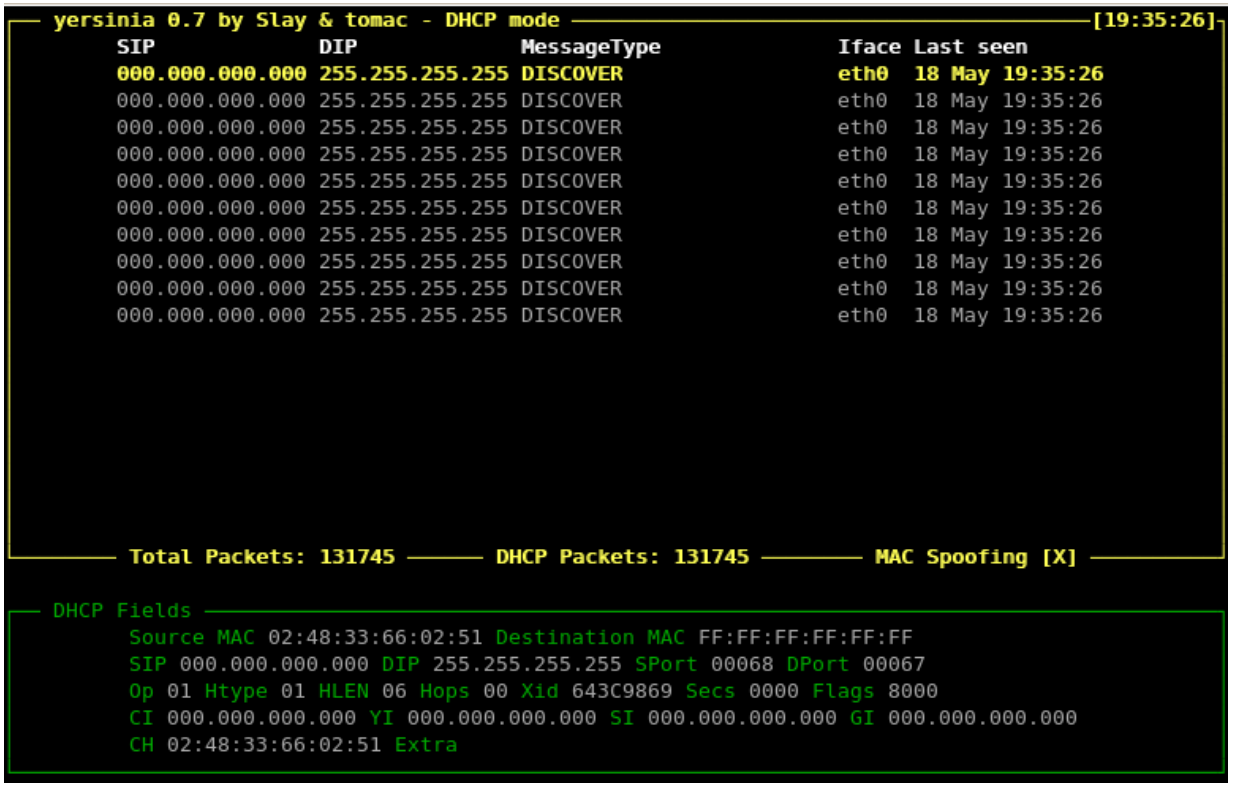


Figura 4-22 Ejecución del ataque 1. Enviando Discovery Packet

```
Switch#show ip dhcp server statistics
Memory usage          7022
Address pools         5
Database agents       0
Automatic bindings    0
Manual bindings       2
Expired bindings      0
Malformed messages    1

Message               Received
BOOTREQUEST           0
DHCPDISCOVER          26003
DHCPREQUEST           0
DHCPDECLINE           0
DHCPRELEASE           0
DHCPINFORM            0

Message               Sent
BOOTREPLY             0
DHCPOFFER             0
DHCPACK               0
DHCPNAK               0
Switch#show ip dhcp server statistics
% The DHCP database could not be locked. Please retry the command later.
Switch#
Switch#
```

Figura 4-23 Denegación del servicio

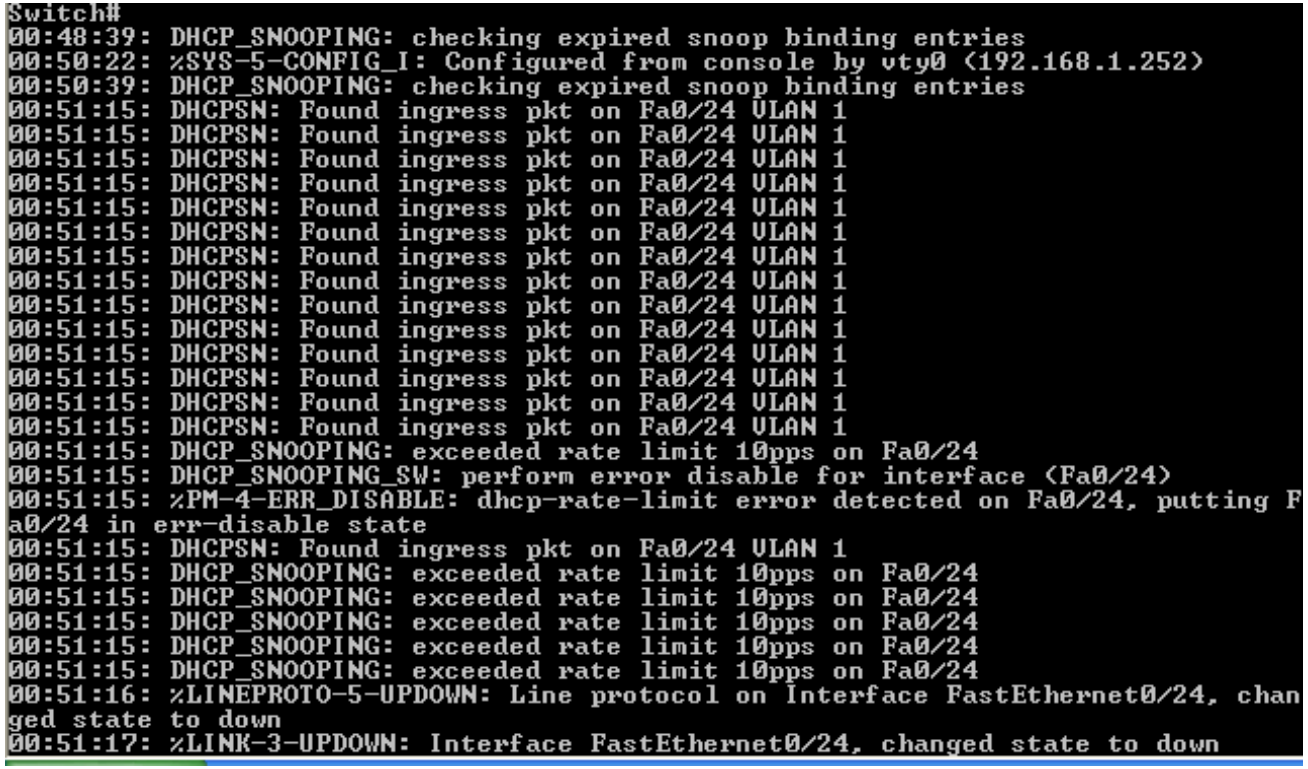


Figura 4-24 Bloqueo del ataque DHCP

4.3.3.2 MAC Spoofing

El método utilizado por los switches para rellenar la tabla de direcciones MAC da lugar a una vulnerabilidad conocida como MAC spoofing. Este tipo de ataque permite a un atacante recibir el tráfico destinado a un host conectado en otro puerto del switch.

El atacante envía paquetes modificando la dirección MAC de su equipo para que coincida con otra dirección MAC conocida de un host objetivo, y tras enviar un frame a toda la red con la dirección MAC que acaba de configurar, el switch aprende que el host objetivo se encuentra en el mismo puerto que el atacante, es decir, asigna la dirección MAC para el nuevo puerto. Como consecuencia todos los paquetes destinados al host objetivo son enviados por el puerto del atacante, aunque otro de los objetivos puede ser conseguir detener el tráfico (DoS o Denegación de Servicio).

En el ejemplo, el switch tiene asociado los puertos 1 y 2 con las direcciones MAC de los dispositivos, por lo que el tráfico destinado a cada dispositivo será directamente enviado.

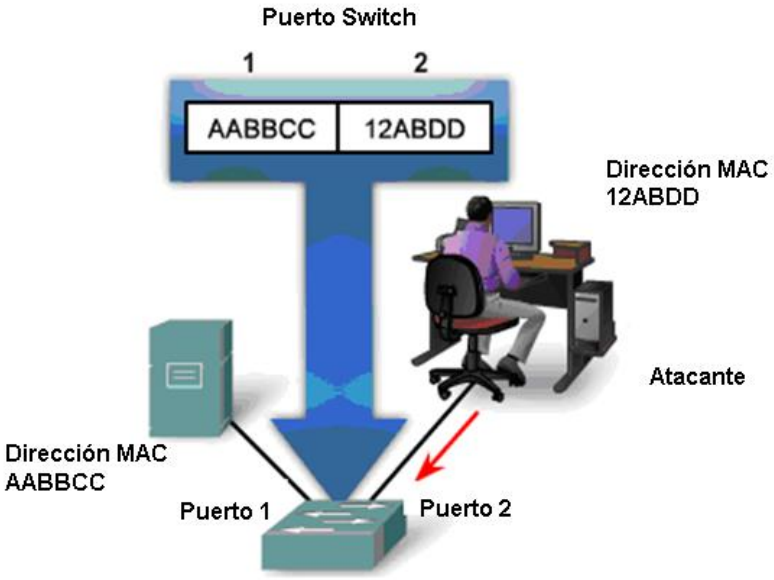


Figura 4-25 Ataque MAC Spoofing

La siguiente figura ilustra como el atacante cambia su dirección MAC por la del host atacado, por lo que el dispositivo con dirección MAC AABBCC es trasladado en la tabla MAC al puerto 2.

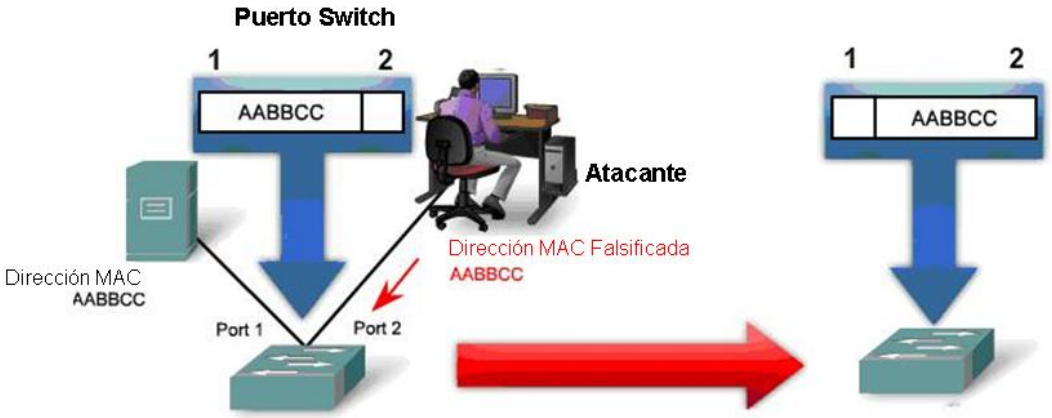


Figura 4-26 Falsificación de dirección MAC

El atacante "toma prestada" la dirección MAC del destinatario como suya propia, sin embargo, cuando el verdadero poseedor de la MAC vuelva a enviar tráfico, se reestablecería su dirección en el puerto correcto. Aún así, no deja de ser una amenaza para la organización, puesto que aunque el problema se corrige a sí mismo, este ataque interrumpe el flujo normal del tráfico y permite al atacante capturar información que iba destinada intencionalmente a otro host.

Este tipo de ataques también se utilizan para saltar la seguridad donde los privilegios van ligados a una dirección MAC, por ejemplo para obtener la dirección IP para acceder al sistema.

Para llevar a cabo este tipo de ataque se pueden utilizar programas como "SMAC", que falsifican direcciones MAC de origen en el S.O., aunque ya el propio sistema operativo permite esta opción en equipos con Windows XP y Linux.

Para mitigar este tipo de ataques, al igual que con el ataque MAC Flooding, un administrador puede configurar un switch Catalyst con seguridad en puerto, en esta ocasión con la opción "sticky". De esta manera aprenderá dinámicamente las direcciones MAC conectadas a sus puertos. Estas direcciones MAC aprendidas se añaden a la running-configuration del switch, lo cual impide que un atacante intente hacer spoofing de una dirección previamente aprendida.

La Tabla 4-6 resume los principales puntos sobre el ataque MAC Spoofing y las pruebas realizadas. Se puede observar que se han definido dos escenarios de pruebas, el primero de ellos, demuestra en la práctica que en una red no segura un atacante alcanza su objetivo, mientras el segundo de los escenarios, demuestra como llevando previamente a cabo las medidas necesarias se consigue mitigar el ataque.

En primer lugar se ha definido una topología para las pruebas, como ilustra la Figura 4-27, donde el atacante es el Host 192.168.1.99 y la victima el Host 192.168.1.7. Un tercer equipo, el Host 192.168.1.252, que está en la interfaz Fa0/2, se utilizará para intentar hacer ping a la

victima una vez se haya lanzado el ataque. En esta misma figura, se puede observar como en la tabla CAM del switch, antes del ataque, el infiltrado está en la interfaz Fa0/14 y la victima en la interfaz Fa0/2.

En el escenario de red no segura, si el Host 192.168.1.99 lanza el ataque, cambiando su dirección MAC como se explica en la Figura 4-28, la tabla CAM del switch refleja el estado mostrado en la Figura 4-29, donde se puede apreciar que la MAC de la victima se ha colocado en la interfaz Fa0/14, la del atacante. Si ahora, el Host 192.168.1.252 intenta establecer comunicación con la victima es imposible, como demuestra la Figura 4-30.

La siguiente prueba consiste en repetir un proceso similar, tras previamente haber configurado en el switch seguridad en puerto. El resultado obtenido ha sido el equivalente al mostrado en las Figura 4-8 , Figura 4-9 y Figura 4-10 para el ataque MAC Flooding. Una vez producida la violación del puerto, el switch deshabilita la boca y la pone en estado err-disable. Inmediatamente, este suceso queda registrado en el servidor Syslog y en Nagios, quien además alerta al administrador de la red mediante un correo.

Ataque MAC Spoofing				
Requerimiento:			➢ **REQ_11**: El administrador de red debe asegurar que los usuarios no puedan cambiar la dirección MAC de su equipo ni que ésta pueda ser suplantada.	
Consecuencias de este ataque:			▪ Pérdidas del servicio ▪ El atacante puede obtener privilegios que van ligados a la dirección MAC.	
Software utilizado:			Sistema operativo	
Procedimiento para mitigar este ataque:			Configurar en el dispositivo la seguridad en Puerto con la opción "Sticky". De esta manera aprenderá dinámicamente las direcciones MAC conectadas a sus puertos, y se añadirán a la running-configuration del switch, impidiendo así que un atacante pueda hacer spoofing de una dirección previamente aprendida.	
Alarmas:			-----	
Pasos			**Instrucciones**	**Referencias**
Escenario 1: Red No Segura	**1**	Lanzar ataque	El atacante cambia su dirección MAC	Figura 4-27 Topología de pruebas para el ataque MAC Spoofing Figura 4-28 Cambio de la MAC
	2	Resultado	El atacante provoca la denegación del servicio y además puede capturar trafico	Figura 4-29 Estado de las tablas CAM Figura 4-30 Denegación de servicio
Escenario 2: Red Segura	**1**	Medidas de mitigación	Configuración en el dispositivo de la seguridad en puerto.	Tratado en Capitulo 6. Seguridad en puerto
	2	Lanzar ataque	El atacante cambia su dirección MAC	Figura 4-27 Topología de pruebas para el ataque MAC Spoofing Figura 4-28 Cambio de la MAC
	3	Resultado	Violación de puerto, la interfaz queda en estado err-disable.	El resultado es el equivalente al mostrado en las Figura 4-8 , Figura 4-9 y Figura 4-10 para el ataque MAC Flooding.

Tabla 4-6 Ataque MAC Spoofing.

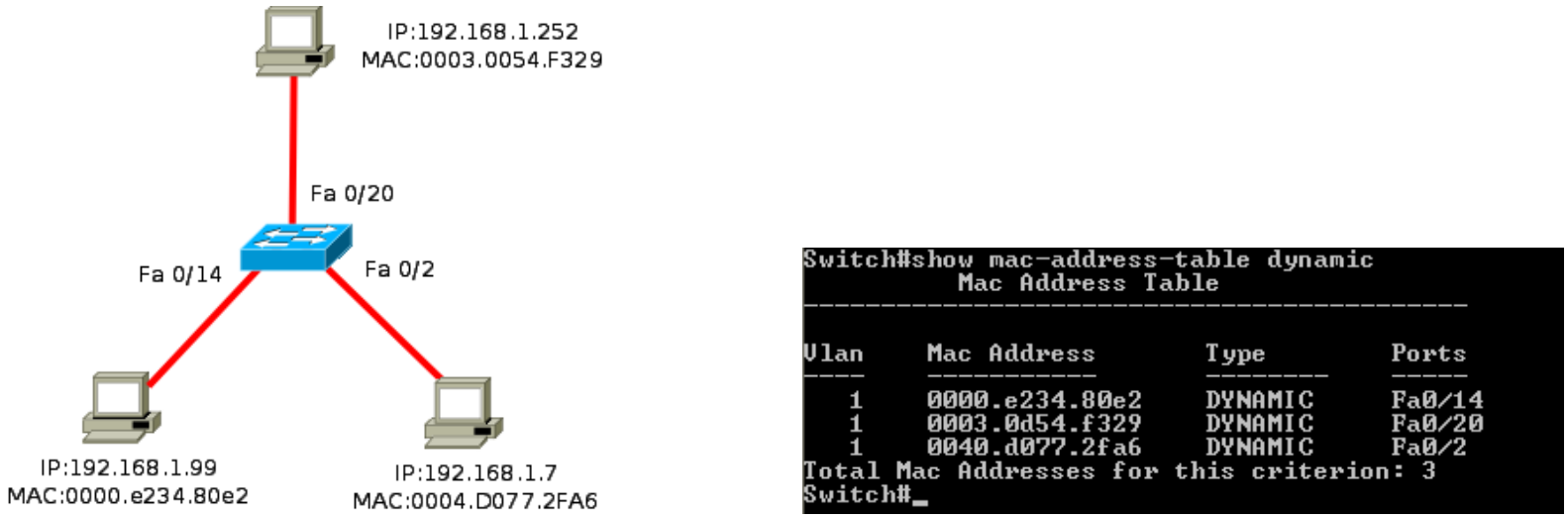


Figura 4-27 Topología de pruebas para el ataque MAC Spoofing

Figura 4-28 Cambio de la MAC

```
Switch#show mac-address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0003.0d54.f329    DYNAMIC     Fa0/20
   1    0040.d077.2fa6    DYNAMIC     Fa0/14
Total Mac Addresses for this criterion: 2
Switch#_
```

Figura 4-29 Estado de las tablas CAM

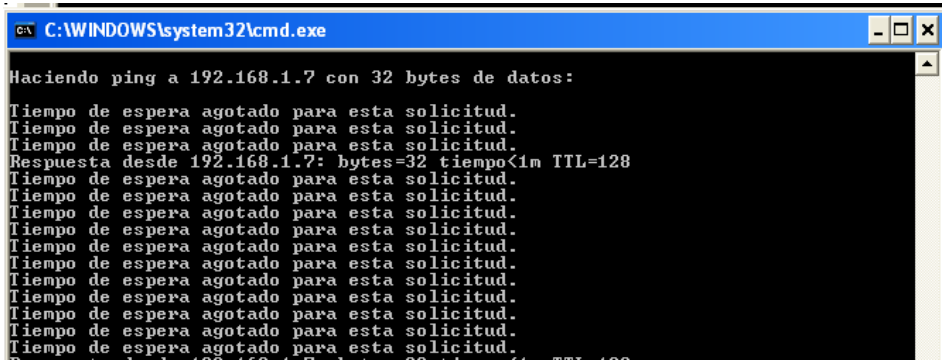


Figura 4-30 Denegación de servicio

4.3.3.3 ARP Spoofing

Una de las técnicas más formidables de ataques internos es la que se denomina ARP spoofing o ARP Poisoning, que coloca a un atacante en una posición en la que puede espiar, y manipular el tráfico local o incluso detenerlo (DoS o Denegación de Servicio). No es fácil de detectar y no hay contramedidas simples.

El ataque consiste en transmitir deliberadamente un paquete ARP falso, conocido como Gratuitous ARP (GARP), cuyo objetivo es manipular o "envenenar" las tablas ARP de otras máquinas, ya que a través de él le estaría indicando a los dispositivos que la MAC del atacante se corresponde con cierta dirección IP.

Cualquier tráfico dirigido a la dirección IP de ese nodo, será erróneamente enviado al atacante, en lugar de a su destino real. El atacante, puede entonces elegir, entre reenviar el tráfico a la puerta de enlace predeterminada real (ataque pasivo o escucha), o modificar los datos antes de reenviarlos (ataque activo). Incluso puede lanzar un ataque de tipo DoS (Denegación de Servicio) contra una víctima, asociando una dirección MAC inexistente con la dirección IP de la puerta de enlace predeterminada de la víctima.

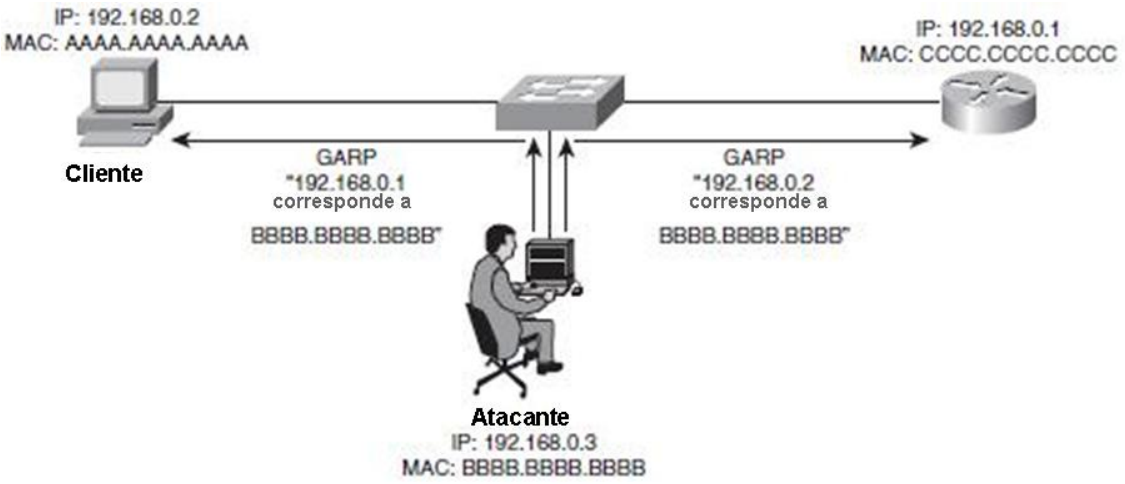


Figura 4-31 Ataque ARP Spoofing

Un método para prevenir el ARP Spoofing, es el uso de tablas ARP estáticas, es decir añadir entradas estáticas ARP, de forma que no exista caché dinámica, cada entrada de la tabla mapea una dirección MAC con su correspondiente dirección IP. Sin embargo, esta no es una solución práctica, sobre todo en redes grandes, debido al enorme esfuerzo necesario para mantener las tablas ARP actualizadas, puesto que cada vez que se cambie la dirección IP de un equipo, es necesario actualizar las tablas de todos los equipos de la red.

Por lo tanto, en redes grandes es preferible usar la característica DHCP Snooping de los switches Cisco, comentada anteriormente. Mediante DHCP, el dispositivo de red mantiene un registro de las direcciones MAC que están conectadas a cada puerto. Esta tabla puede usarse por DAI (Dynamic ARP Inspection) para ayudar a prevenir los ataques por spoofing de ARP, de modo que rápidamente se detecte si se está recibiendo una suplantación ARP.

DAI trabaja de forma similar a DHCP snooping, usando puertos seguros (trusted) e inseguros (untrusted). Las respuestas ARP son permitidas en el switch en puertos seguros. Si una respuesta ARP llega al switch por un puerto inseguro, el contenido de la respuesta se compara con la tabla de vinculaciones DHCP para verificar su fiabilidad. Si no coincide con la tabla, la respuesta ARP se elimina, y el puerto se deshabilita. Otra solución factible es el uso de ARPWatch, que se detalla mas abajo en este mismo capitulo, y es por la que se ha optado en el IATE. Sin embargo, se han realizado pruebas en ambos sentidos.

La Tabla 4-7 recoge la lista de verificación para el ataque ARP Spoofing. Se puede observar que en esta ocasión se han definido tres escenarios de pruebas, el primero de ellos, demuestra en la práctica que en una red no segura un atacante alcanza su objetivo, mientras que los otros escenarios presentan las dos opciones posibles que existen para combatir este ataque, alertar al administrar de la detección del ataque para que pueda actuar a la mayor brevedad o bien directamente mitigarlo.

En primer lugar, en la Figura 4-32 se ha definido una topología para las pruebas, donde el atacante es el Host 192.168.1.99 y la victima el Host 192.168.1.7. Un tercer equipo, el Host 192.168.1.252, tiene instalada una maquina virtual con Centos y ARPWatch. Se añade también un router con salida a Internet con la IP 192.168.1.1

El objetivo de este ataque es envenenar las tablas ARP de la victima, cambiando la MAC de la puerta de enlace por la del atacante. La herramienta utilizada para lanzar el ataque es Cain&Abel. Este software capturará el tráfico que generen los equipos 192.168.1.7 y 192.168.1.252, obteniendo de este modo las credenciales de estos usuarios. Los pasos seguidos con Cain&Abel son:

1. Rastrear las IP del segmento de subred donde se va a realizar el ataque. El resultado obtenido se muestra en la Figura 4-34, y concuerda con el diagrama lógico mostrado en la Figura 4-32 Topología de pruebas para ataque ARP Spoofing.

2. En la Figura 4-35 se ilustra como en la pestaña ARP de Cain&Abel se puede lanzar el ataque ARP Poison. En dicha ventana el atacante debe seleccionar entre que equipos desea situarse para llevar a cabo un ataque del tipo “hombre en el medio”. En esta

misma figura se observa que para esta prueba el atacante está situado entre el router de salida y los equipos de la red, para de este modo capturar todo el tráfico.

Una vez lanzado, el resultado del ataque es el envenenamiento de las tablas ARP con la MAC del infiltrado, como se puede observar en la Figura 4-36 y Figura 4-38. Mientras tanto, el atacante puede ir capturando mediante Cain & Abel las credenciales de los usuarios de los equipos, como demuestra la Figura 4-37.

En el escenario numero 2, la prueba consiste en repetir un proceso similar al anterior, pero tras previamente haber activado ARPWatch. En la Figura 4-39 se recoge la base de datos de ARPWatch, donde aparecen los equipos que se han definido en la topología de red empleada para las pruebas. En esta ocasión, el ARPWatch alerta al administrador ante un cambio del par (MAC, IP). Cuando Cain & Abel modifica la MAC de la puerta de enlace 192.168.1.1, el administrador recibe un correo cuyo contenido es el mostrado en Figura 4-40. De este modo, puede actuar rápidamente, por ejemplo bloqueando la boca, y conseguir que la tabla ARP vuelva al estado inicial, como se demuestra en la Figura 4-41.

En el escenario numero 3, de nuevo se repite un proceso similar, pero esta vez tras previamente haber configurado DAI, el cual necesita de la configuración previa de DHCP Snooping, como puede comprobarse en la Figura 4-42, ya que gracias a la base de datos de DHCP Snooping, DAI comprueba la relación entre la MAC-IP, como hace ARPWatch. Pero además es necesario introducir manualmente las entradas estáticas de los equipos mediante el uso de ACL.

En este último escenario, cuando Cain & Abel intenta envenenar las tablas MAC de los equipos, en este caso la MAC de la puerta de enlace 192.168.1.1, DAI bloquea el ataque, como se muestra en la Figura 4-43. De este modo, las tablas ARP de los equipos atacados no son modificadas, como se refleja en la Figura 4-44.

Sin embargo, después de evaluar ambas opciones, para el IATE se ha optado por el uso de ARPWatch. Se ha descartado DAI debido a que además de requerir una configuración mucho más compleja, su uso provoca un alto consumo de CPU, al estar constantemente comparando las tablas, lo cual puede desencadenar lentitud en la red. El uso de DAI suele estar justificado en las gamas altas de switches de acceso, para empresas con un elevado número de usuarios, que no es el caso del IATE.

<table>
<tr><th colspan="5">Ataque ARP Spoofing</th></tr>
<tr><td colspan="2">Requerimiento:</td><td colspan="3">➢ REQ_12: El administrador debe mitigar los ataques de ARP Spoofing que se produzcan en la red</td></tr>
<tr><td colspan="2">Consecuencias de este ataque:</td><td colspan="3">▪ Denegación del servicio
▪ El atacante puede capturar tráfico de la red.</td></tr>
<tr><td colspan="2">Software utilizado:</td><td colspan="3">Cain & Abel</td></tr>
<tr><td colspan="2">Procedimiento para mitigar este ataque:</td><td colspan="3">Activar ARPWatch para que el administrador de la red sea notificado cuando el ataque es detectado y pueda actuar en consecuencia lo antes posible. Otra opción es configurar DAI.</td></tr>
<tr><td colspan="2">Alarmas:</td><td colspan="3">✓ Correo electrónico</td></tr>
<tr><th colspan="3">Pasos</th><th>Instrucciones</th><th>Referencias</th></tr>
<tr><td rowspan="2">Escenario 1: Red No Segura</td><td>1</td><td>Lanzar ataque</td><td>Se lanza el ataque mediante el software Cain & Abel</td><td>Figura 4-32 Topología de pruebas para ataque ARP Spoofing
Figura 4-33 Tabla ARP del equipo
Figura 4-34 Cain & Abel. Rastreo de equipos en el segmento de red.
Figura 4-35 Cain & Abel. Lanzar ataque ARP Poison</td></tr>
<tr><td>2</td><td>Resultado</td><td>Obtención de credenciales de la victima.</td><td>Figura 4-36 Cain & Abel. Envenenamiento de las tablas ARP
Figura 4-37 Cain & Abel. Obtención de credenciales
Figura 4-38 Tabla ARP envenenada en el equipo victima</td></tr>
<tr><td rowspan="3">Escenario 2: Red Segura</td><td>1</td><td>Medidas de mitigación</td><td>Activar arpwatch. En el servidor tiene que estar levantado el servicio de ARPWatch</td><td>Figura 4-39 Base de datos de ARPWatch</td></tr>
<tr><td>2</td><td>Lanzar ataque</td><td>Se lanza el ataque mediante el software Cain & Abel</td><td>Figura 4-32 Topología de pruebas para ataque ARP Spoofing
Figura 4-33 Tabla ARP del equipo
Figura 4-34 Cain & Abel. Rastreo de equipos en el segmento de red.
Figura 4-35 Cain & Abel. Lanzar ataque ARP Poison</td></tr>
<tr><td>3</td><td>Resultado</td><td>El administrador de red es notificado del ataque para que pueda tomar medidas.</td><td>Figura 4-36 Cain & Abel. Envenenamiento de las tablas ARP
Figura 4-40 Correo enviados por ARPWatch
Figura 4-41 Tabla ARP una vez mitigado el ataque</td></tr>
</table>

Escenario 3: Red Segura	**1**	Medidas de mitigación	Configuración de DAI.	Tratado en Capitulo 6. Configuración de DAI. Figura 4-42 Base de datos de DHCP Snooping
	2	Lanzar ataque	Se lanza el ataque mediante el software Cain & Abel	Figura 4-32 Topología de pruebas para ataque ARP Spoofing Figura 4-33 Tabla ARP del equipo Figura 4-34 Cain & Abel. Rastreo de equipos en el segmento de red. Figura 4-35 Cain & Abel. Lanzar ataque ARP Poison
	3	Resultado	Se bloquea el ataque y se registra una notificación en SysLog	Figura 4-36 Cain & Abel. Envenenamiento de las tablas ARP Figura 4-43 Notificación Syslog debido al bloqueo del ataque con DAI Figura 4-44 Tabla ARP del equipo atacado

Tabla 4-7 Ataque ARP Spoofing.

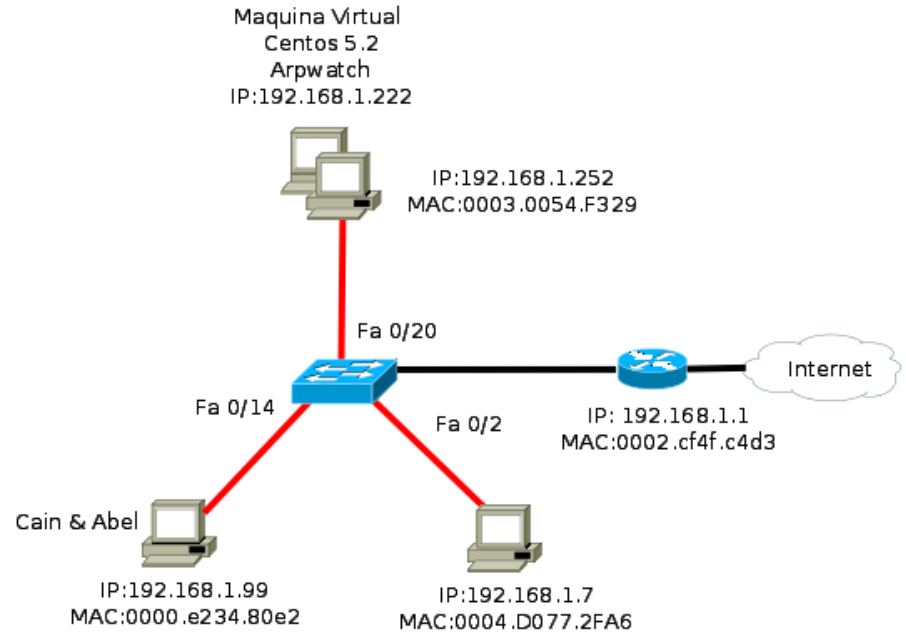
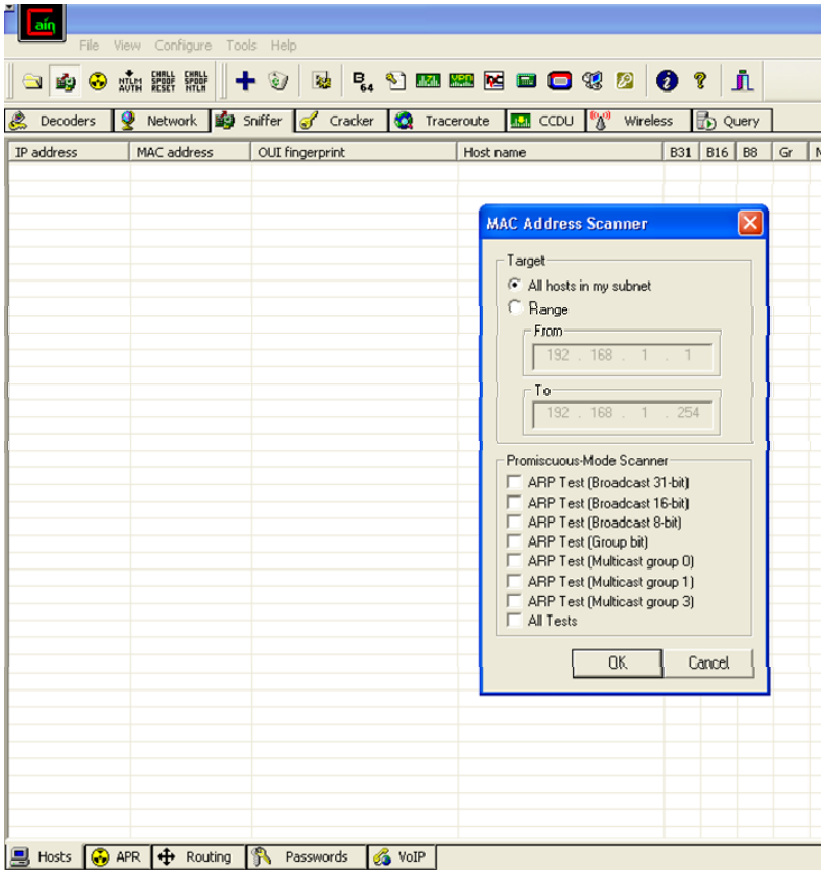


Figura 4-32 Topología de pruebas para ataque ARP Spoofing

```
C:\Documents and Settings\emilio>arp -a

Interfaz: 192.168.1.252 --- 0x4
  Dirección IP          Dirección física      Tipo
  192.168.1.1           00-02-cf-4f-c4-d3     dinámico
```

Figura 4-33 Tabla ARP del equipo



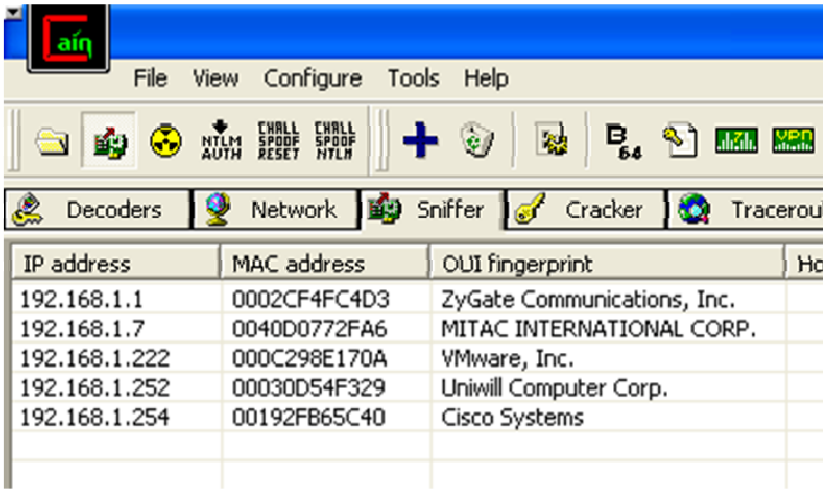


Figura 4-34 Cain & Abel. Rastreo de equipos en el segmento de red.

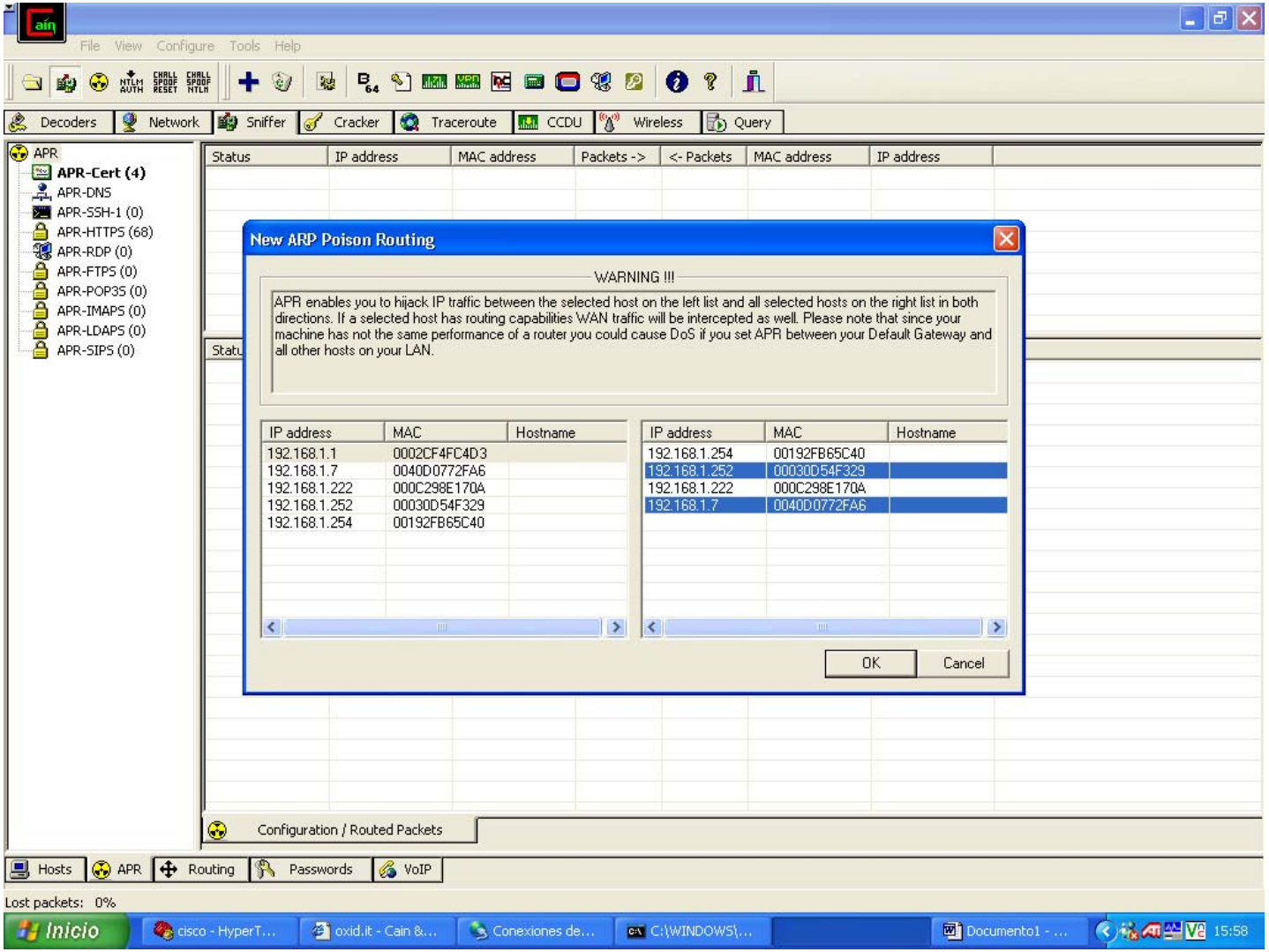


Figura 4-35 Cain & Abel. Lanzar ataque ARP Poison

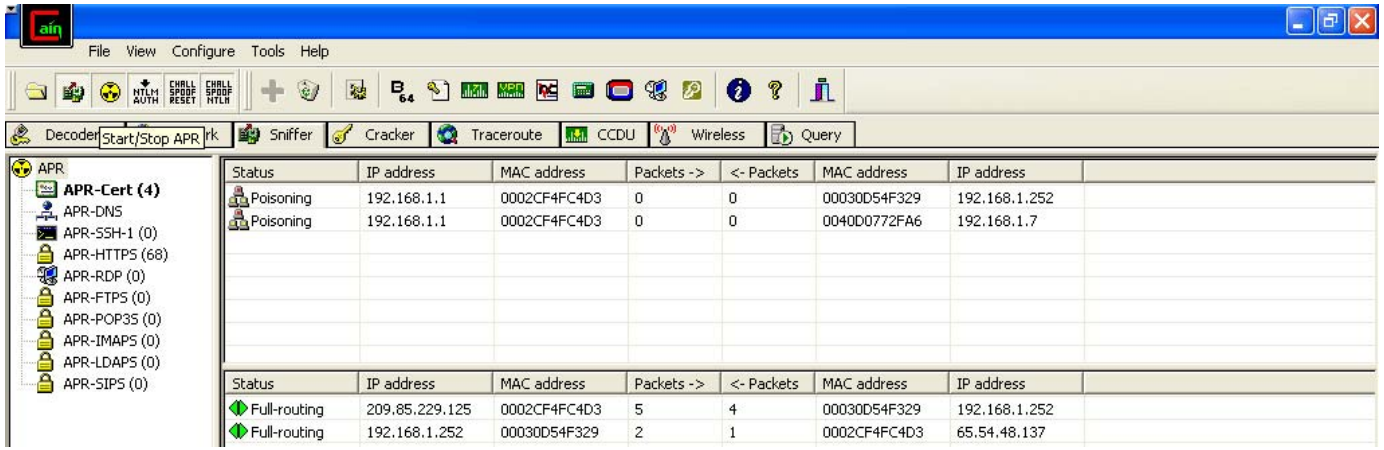


Figura 4-36 Cain & Abel. Envenenamiento de las tablas ARP

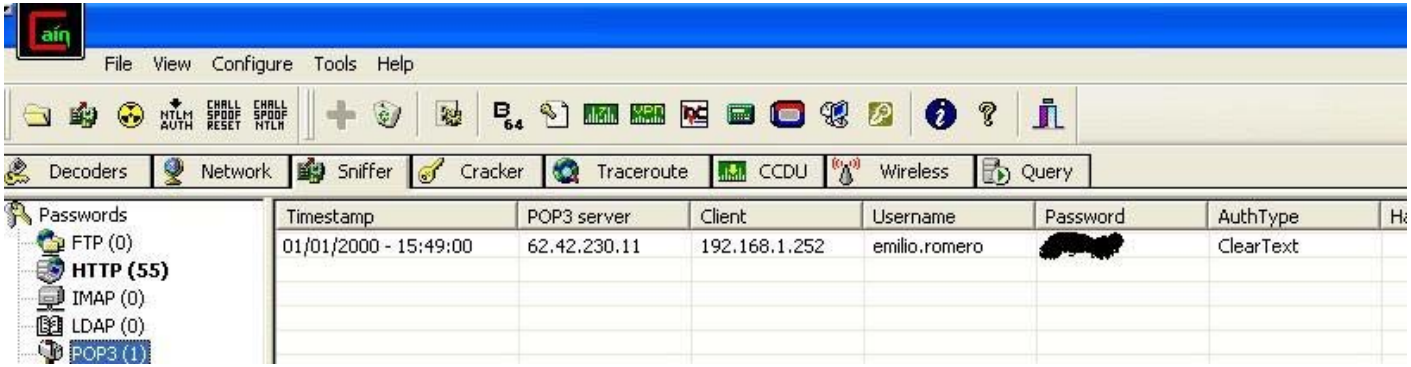


Figura 4-37 Cain & Abel. Obtención de credenciales

```
C:\Documents and Settings\emilio>arp -a

Interfaz: 192.168.1.252 --- 0x4
  Dirección IP          Dirección física      Tipo
  192.168.1.1           00-00-e2-34-80-e2     dinámico
```

Figura 4-38 Tabla ARP envenenada en el equipo victima

```
[root@ingenia arpwatch]# cat arp.dat
0:c:29:8e:17:a  192.168.1.222   1274612545
0:3:d:54:f3:29  192.168.1.252   1274612536
0:19:2f:b6:5c:40        192.168.1.254   1274612549      ScSwitch11
0:2:cf:4f:c4:d3 192.168.1.1     1274612545
0:0:e2:34:80:e2 192.168.1.99    1274612266
0:40:d0:77:2f:a6        192.168.1.7     1274612387
[root@ingenia arpwatch]#
```

root@ingenia:/var/arpwatch

Figura 4-39 Base de datos de ARPWatch

Arpwatch para usuario mostrar detalles 23 may

hostname: <unknown>
ip address: 192.168.1.1
ethernet address: 0:2:cf:4f:c4:d3
ethernet vendor: ZyGate Communications, Inc.
old ethernet address: 0:0:e2:34:80:e2
old ethernet vendor: ACER TECHNOLOGIES CORP.
timestamp: Sunday, May 23, 2010 13:31:38 +0200
previous timestamp: Sunday, May 23, 2010 13:31:17 +0200
delta: 21 seconds

Arpwatch para usuario mostrar detalles 23 may

hostname: <unknown>
ip address: 192.168.1.1
ethernet address: 0:0:e2:34:80:e2
ethernet vendor: ACER TECHNOLOGIES CORP.
old ethernet address: 0:2:cf:4f:c4:d3
old ethernet vendor: ZyGate Communications, Inc.
timestamp: Sunday, May 23, 2010 13:31:39 +0200
previous timestamp: Sunday, May 23, 2010 13:31:38 +0200
delta: 1 second

Arpwatch para usuario mostrar detalles 23 may

hostname: <unknown>
ip address: 192.168.1.1
ethernet address: 0:2:cf:4f:c4:d3
ethernet vendor: ZyGate Communications, Inc.
old ethernet address: 0:0:e2:34:80:e2
old ethernet vendor: ACER TECHNOLOGIES CORP.
timestamp: Sunday, May 23, 2010 13:31:41 +0200
previous timestamp: Sunday, May 23, 2010 13:31:39 +0200
delta: 2 seconds

Figura 4-40 Correo enviados por ARPWatch

```
nterfaz: 192.168.1.252 --- 0x4
 Dirección IP          Dirección física      Tipo
 192.168.1.1           00-02-cf-4f-c4-d3     dinámico
 192.168.1.99          00-00-e2-34-80-e2     dinámico
```

Figura 4-41 Tabla ARP una vez mitigado el ataque

```
ScSwitch01#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:03:0D:54:F3:29   192.168.1.252    85076       dhcp-snooping   10    FastEthernet0/20
00:40:D0:77:2F:A6   192.168.1.7      86291       dhcp-snooping   10    FastEthernet0/2
00:00:E2:34:80:E2   192.168.1.99     85776       dhcp-snooping   10    FastEthernet0/14
Total number of bindings: 3
```

Figura 4-42 Base de datos de DHCP Snooping

```
001228: *Mar  1 03:54:56: %SYS-5-CONFIG_I: Configured from console by console
001229: *Mar  1 03:54:57: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/14, changed state to up[OK]
ScSwitch01#
001230: *Mar  1 03:54:59: %LINK-3-UPDOWN: Interface FastEthernet0/14, changed state to up
001231: *Mar  1 03:55:52: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/14, vlan 10.([0000.e234.80e2/192.168.1.25
2/0002.cf4f.c4d3/192.168.1.1/03:55:51 UTC Mon Mar 1 1993])
001232: *Mar  1 03:55:52: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/14, vlan 10.([0000.e234.80e2/192.168.1.1/
0003.0d54.f329/192.168.1.252/03:55:51 UTC Mon Mar 1 1993])
001233: *Mar  1 03:56:12: %SW_DAI-4-INVALID_ARP: 2 Invalid ARPs (Req) on Fa0/14, vlan 10.([0003.0d54.f329/192.168.1.252/0000.
0000.0000/192.168.1.1/03:56:11 UTC Mon Mar 1 1993])
001234: *Mar  1 03:56:12: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Fa0/14, vlan 10.([0002.cf4f.c4d3/192.168.1.1/
0000.0000.0000/192.168.1.252/03:56:11 UTC Mon Mar 1 1993])
001235: *Mar  1 03:56:50: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/14, vlan 10.([0000.e234.80e2/192.168.1.25
2/0000.0000.0000/192.168.1.1/03:56:50 UTC Mon Mar 1 1993])
001236: *Mar  1 03:56:50: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/14, vlan 10.([0000.e234.80e2/192.168.1.1/
0000.0000.0000/192.168.1.252/03:56:50 UTC Mon Mar 1 1993])
001237: *Mar  1 03:56:50: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/14, vlan 10.([0000.e234.80e2/192.168.1.7/
0000.0000.0000/192.168.1.1/03:56:50 UTC Mon Mar 1 1993])
001238: *Mar  1 03:56:50: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/14, vlan 10.([0000.e234.80e2/192.168.1.1/
0000.0000.0000/192.168.1.7/03:56:50 UTC Mon Mar 1 1993])
001239: *Mar  1 03:56:50: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/14, vlan 10.([0000.e234.80e2/192.168.1.25
2/0013.1a66.eb80/192.168.1.1/03:56:50 UTC Mon Mar 1 1993])
001240: *Mar  1 03:56:50: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/14, vlan 10.([0000.e234.80e2/192.168.1.1/
0003.0d54.f329/192.168.1.252/03:56:50 UTC Mon Mar 1 1993])
001241: *Mar  1 03:56:50: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/14, vlan 10.([0000.e234.80e2/192.168.1.7/
0013.1a66.eb80/192.168.1.1/03:56:50 UTC Mon Mar 1 1993])
001242: *Mar  1 03:56:50: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/14, vlan 10.([0000.e234.80e2/192.168.1.1/
0040.d077.2fa6/192.168.1.7/03:56:50 UTC Mon Mar 1 1993])
```

Figura 4-43 Notificación Syslog debido al bloqueo del ataque con DAI

```
C:\Documents and Settings\emilio>arp -a

Interfaz: 192.168.1.252 --- 0x4
  Dirección IP          Dirección física      Tipo
  192.168.1.1           00-02-cf-4f-c4-d3     dinámico
  192.168.1.7           00-40-d0-77-2f-a6     dinámico
  192.168.1.99          00-00-e2-34-80-e2     dinámico
```

Figura 4-44 Tabla ARP del equipo atacado

4.3.3.4 Ataques STP

Como se vio en el capítulo anterior, STP permite la existencia de enlaces físicos redundantes, eliminando de forma lógica los bucles de conmutación, gracias a la implementación de una topología en forma de árbol lógico, que permite coordinar la comunicación entre los switches con el fin de evitar los bucles. Pues bien, el equipo atacante buscará convertirse en la raíz de dicho árbol, con el objetivo de acceder a los paquetes de información que circulan por todos los switches.

Si un atacante tiene acceso a un puerto del switch, puede introducir un switch infiltrado en la red y configurarlo con una prioridad de puente menor para que se convierta en puente raíz. Tras inundar de BPDUs que indiquen que él es el switch con el BID más bajo, la topología STP re-convergerá. Gracias a esto, ahora todo el tráfico pasará a través del switch infiltrado y el atacante podrá capturarlo.

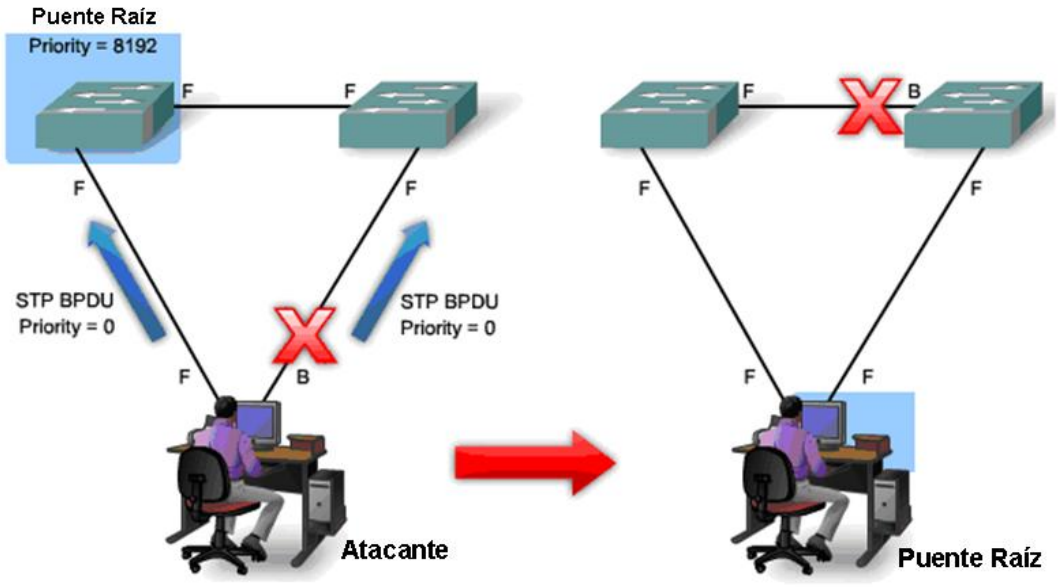


Figura 4-45 Ataque STP

Existen 2 enfoques para proteger a la red contra este tipo de ataque:

- ✓ Protección con “Root Guard”. Esta solución permite participar en el proceso de STP pero no la entrada de BPDU que indiquen un mejor BID. En tal caso, el puerto cambia al estado “root-inconsistent “, impidiendo que puedan fluir datos de usuario a través de él. Cuando cese la recepción de dicha BPDU, el puerto volverá al estado de envío.

- ✓ Protección con “BPDU Guard”. Configurada en puertos PortFast. Es una solución más radical que no permite ningún tráfico de BPDU. Si un puerto configurado con BDPU Guard recibe una BPDU, el puerto quedará deshabilitado.

La Tabla 4-8 recoge la lista de verificación para el ataque STP. Se puede observar que se han definido dos escenarios de pruebas, el primero de ellos, demuestra en la práctica que en una red no segura un atacante alcanza su objetivo, mientras el segundo de los escenarios, demuestra como llevando previamente a cabo las medidas necesarias se consigue mitigar el ataque.

En primer lugar se comprueba que el switch empleado para las pruebas es el puente raíz, como se observa en la Figura 4-46 mediante el texto “This bridge is the root”

La Figura 4-47 presenta los diferentes tipos de ataques STP que permite ejecutar Yersina, tanto de denegación de servicio como de suplantación del puente raíz. Los ataques 2 y 3 (Sending Conf BPDUs y Sending TCN BPDUs respectivamente) pueden provocar la caída completa de la red. Estos ataques fuerzan que los switch estén continuamente recalculando sus caminos.

Comenzando por el escenario de red no segura, se lanza con Yersina el ataque 4 (Claiming Root Role), como se explica en la Figura 4-48, que permite al atacante conseguir el rol de puente raíz mediante el envío de un BID menor que el actual BID del nodo raíz de la red, como demuestra la Figura 4-49.

La siguiente prueba consiste en repetir un proceso similar, tras previamente haber configurado PortFast y BDPU Guard en la interfaz 0/20, como se puede ver en la Figura 4-50. De nuevo, se lanza con Yersina el ataque 4 (Claiming Root Role), pero esta vez, el switch pone al puerto en estado err-disable, de forma que el ataque no tiene éxito, como se puede comprobar en la Figura 4-51.

Ataque STP				
Requerimiento:			➢ **REQ_13**: El administrador de red debe asegurar la integridad del puente raíz.	
Consecuencias de este ataque:			El atacante buscará convertirse en la raíz del árbol, con el objetivo de acceder a los paquetes de información que circulan por todos los switches.	
Software utilizado:			Yersinia	
Procedimiento para mitigar este ataque:			Existen dos enfoques para proteger a la red contra este tipo de ataque: Protección con "Root Guard", que permite participar en el proceso de STP pero no la entrada de BPDU que indiquen un mejor BID; Protección con "BPDU Guard", configurada en puertos PortFast, solución más radical que no permite ningún tráfico de BDPU. En el IATE se ha optado por la última de las opciones.	
Alarmas:			-----	
Pasos			**Instrucciones**	**Referencias**
Escenario 1: Red No Segura	**1**	Lanzar ataque	Se lanza el ataque mediante el software Yersinia	Figura 4-46 Puente raíz Figura 4-47 Yersina. Tipos de ataques STP Figura 4-48 Ataque tipo 4. Claiming Root Role
	2	Resultado	El atacante consigue convertirse en el puente raíz	Figura 4-49 Pérdida del Rol de Root
Escenario 2: Red Segura	**1**	Medidas de mitigación	Se configura PortFast en las bocas donde se va a conectar los equipos finales, y se configura BDPU Guard	Tratado en Capitulo 6. Configuración de Portfast/BDPU Guard Figura 4-50 Configuración de PortFast y BDPU Guard
	2	Lanzar ataque	Se lanza el ataque mediante el software Yersinia	Figura 4-46 Puente raíz Figura 4-47 Yersina. Tipos de ataques STP Figura 4-48 Ataque tipo 4. Claiming Root Role
	3	Resultado	El puerto del switch se bloquea y queda en estado err-disable.	Figura 4-51 BDPU Guard bloquea el ataque STP

Tabla 4-8 Ataque STP.

```
Switch#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    24577
              Address     0013.1a66.eb80
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     0013.1a66.eb80
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/20           Desg FWD 19        128.20   P2p
```

Figura 4-46 Puente raíz

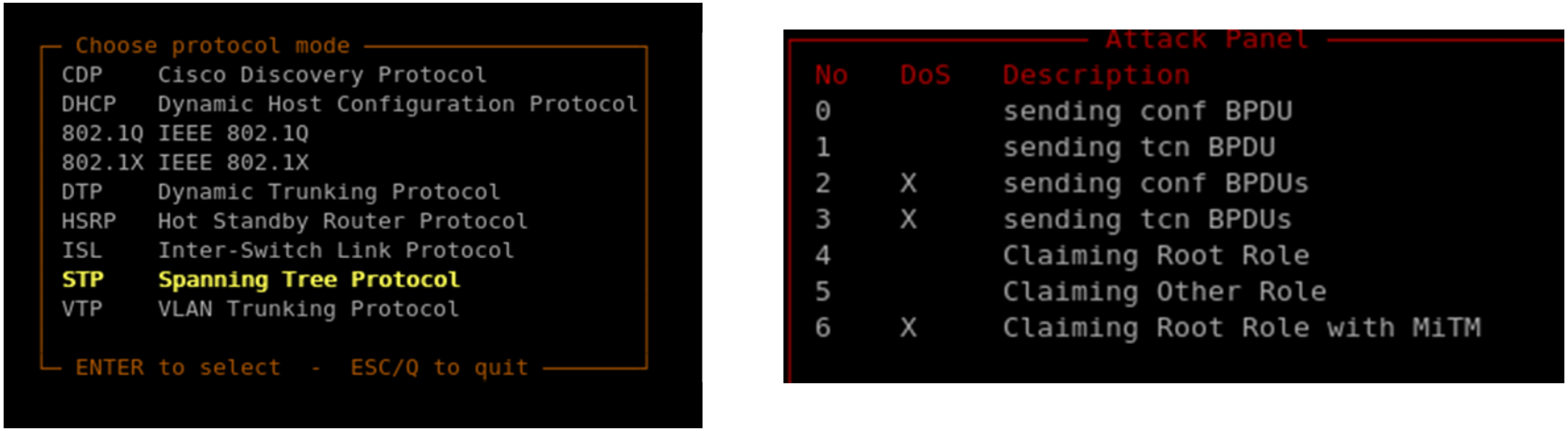


Figura 4-47 Yersina. Tipos de ataques STP

Figura 4-48 Ataque tipo 4. Claiming Root Role

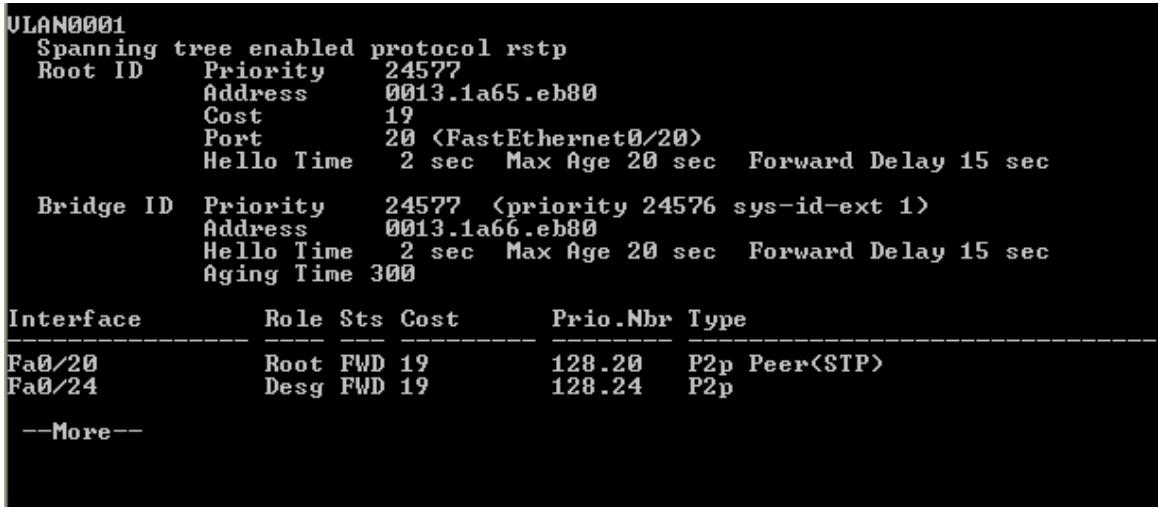


Figura 4-49 Pérdida del Rol de Root

```
Switch#show running-config interface fastEthernet 0/20
Building configuration...

Current configuration : 114 bytes
!
interface FastEthernet0/20
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
end

Switch#
```

Figura 4-50 Configuración de PortFast y BDPU Guard

```
Switch#
00:58:44: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/20, chan
ged state to up
Switch#
00:58:46: %LINK-3-UPDOWN: Interface FastEthernet0/20, changed state to up
00:58:46: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port FastEthernet0/20 wi
th BPDU Guard enabled. Disabling port.
00:58:46: %PM-4-ERR_DISABLE: bpduguard error detected on Fa0/20, putting Fa0/20
in err-disable state
00:58:47: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/20, chan
ged state to down
00:58:48: %LINK-3-UPDOWN: Interface FastEthernet0/20, changed state to down
```

Figura 4-51 BDPU Guard bloquea el ataque STP

4.3.4 Enfoques básicos para proteger los switches de capa 2

A modo de resumen, este apartado recoge una serie de recomendaciones finales con el fin de defender a los switches de capa 2 de los ataques anteriormente descritos. Es evidente que todas ellas se aplicarán en el IATE.

- SNMP es un protocolo usado a menudo para obtener información sobre dispositivos de red. Las versiones 1 y 2 de este protocolo no tienen mecanismos de seguridad sólidos, por lo que si se usan, es recomendable considerar permitir SNMP con accesos de sólo lectura, en lugar de lectura y escritura. De forma alternativa, considerar utilizar SNMPv3.

- Deshabilitar todos los servicios innecesarios en el switch y configurar los puertos del switch en modo acceso, deshabilitando DTP en todos los puertos que no necesiten formar un enlace troncal.

- No enviar datos de usuario sobre una VLAN nativa en un troncal 802.1Q y añadir todos los puertos no utilizados a una VLAN sin uso y deshabilitarlos.

- Usar mecanismos de protección STP como Root guard y BPDU Guard.

- La implementación de banners que prohíban el acceso no autorizado.

- Para combatir los ataques tanto por “envenenamiento” como por “agotamiento” habilitar DHCP Snooping y DAI.

- Limitar el número de MACs que un puerto puede aprender mediante la configuración de seguridad en puerto.

- Otra práctica recomendada es revisar de forma regular los log del switch, ya que puede alertar sobre amenazas potenciales.

- Registrar (syslog) los intentos de acceso no autorizados y revisar los registros periódicamente.

- También se puede mejorar la seguridad estableciendo un Time-out de inactividad.

4.4 Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) son mecanismos opcionales en el software IOS Cisco, que pueden configurarse para filtrar o comprobar paquetes, y determinar así si deben reenviarse a su destino o descartarse.

Al crear listas de control de acceso, el administrador de red tiene varias opciones. La complejidad de las pautas de diseño determina el tipo de ACL necesaria.

- **ACL estándar**. Es la más simple. Las ACLs IP estándar filtran según la dirección IP de origen de un paquete y permiten o deniegan el acceso de acuerdo con la totalidad del protocolo IP. De esta manera, si un dispositivo host es denegado por una ACL estándar, se deniegan todos los servicios provenientes de ese host. Este tipo de ACL sirve para permitir el acceso de todos los servicios de un usuario específico o LAN, a través de un router, y a la vez, denegar el acceso de otras direcciones IP. Las ACL estándar están identificadas por el número que se les ha asignado. Para las listas de acceso que permiten o deniegan el tráfico IP, el número de identificación puede variar entre [1- 99] y [1300- 1999].

- **ACL extendidas.** Filtran no sólo según la dirección IP de origen, sino también según la dirección IP del destino, el protocolo y los números de puertos. Se utilizan más que las ACL estándar porque son más específicas y ofrecen un mayor control. El rango de números de las ACL extendidas varia entre [100- 199] y [2000- 2699]

- **ACL nombradas (NACL, Named ACL).** Son ACL estándar o extendidas a las que se hace referencia mediante un nombre descriptivo en lugar de un número.

Además los switches de capa 3 admiten dos tipos más de ACLs, como son RACL y VACL.

- **Router access control list (RACL).** Son aplicadas a las SVI del switch o a los puertos enrutados de capa 3. Controla el acceso del tráfico enrutado entre las VLAN y se aplican en las interfaces para permitir o denegar el tráfico entrante o saliente.

- **VLAN access control list (VACL).** Filtran el tráfico basado en capa 2 o 3, dentro de la misma VLAN. No están definidas por dirección del trafico (Entrada o salida).

La Figura 4-52 ofrece un ejemplo de RACL y VACL. Como se puede observar, siguiendo la línea amarilla, el tráfico generado desde la VLAN 10 a la VLAN 20 puede ser enrutado por una lista de control de acceso del tipo RACL.

En cambio la VACL controla el tráfico dentro de la VLAN, por lo que el tráfico generado en el switch no llega al router. En caso de querer bloquear el tráfico dentro de la VLAN 10 habría que utilizar VACL.

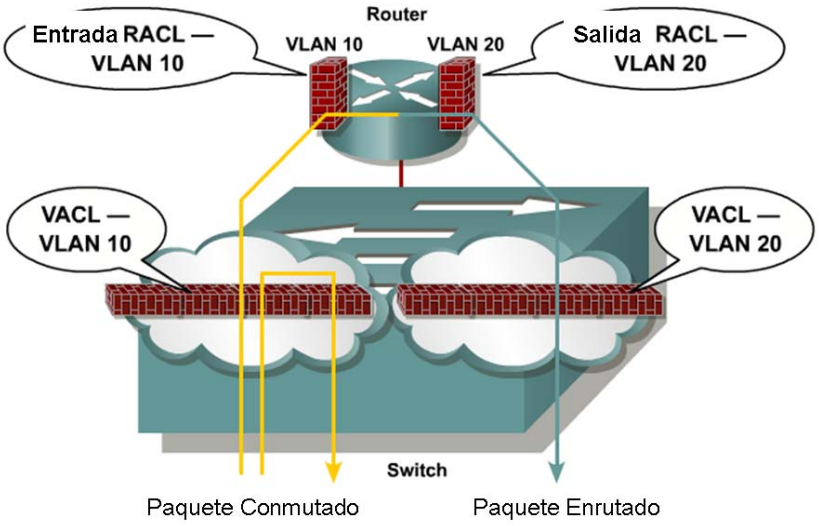


Figura 4-52 RACLs y VACLs

En el IATE se van a utilizar las ACLs para permitir o denegar el acceso por SSH, tanto de los switch como de los servidores.

A continuación se incluye la lista de verificación que garantiza que se han cubierto todos los requisitos del cliente relacionados con las listas de control de acceso.

Lista de verificación para ACLs			
Requerimiento:	El administrador de red debe asegurar que: ➢ **REQ_14**: El acceso a la línea de la terminal solo se puede realizar desde la VLAN de informática. ➢ **REQ_15**: Ningún usuario no autorizado accede a la VLAN de administración ➢ **REQ_16**: Ningún usuario no autorizado accede por ssh a los servidores ➢ **REQ_17**: Las VLANs de los usuarios no se verán entre sí.		
Procedimiento:	▪ **Para REQ_14**: Configurar una VLAN estándar que solo permita el acceso a la línea de terminal desde la VLAN de informática ▪ **Para REQ_15**: Configurar RACL para permitir el acceso a la VLAN de administración solo desde la VLAN de informática ▪ **Para REQ_16:** Configurar RACL para permitir el acceso a la VLAN de servidores solo desde la VLAN de informática ▪ **Para REQ_17:** Configurar RACL para que las VLANs de los usuarios no puedan verse entre sí.		
Pasos		**Instrucciones**	**Estado**
REQ_14	**1**	Crear una ACL estándar	Realizado
	2	Aplicar a la línea de terminal VTY 0 15	Realizado
REQ_15	**1**	Crear una RACL	Realizado
	2	Aplicar la RACL a la VLAN	Realizado
REQ_16	**1**	Crear una RACL	Realizado
	2	Aplicar la RACL a la VLAN	Realizado
REQ_17	**1**	Crear una RACL	Realizado
	2	Aplicar la RACL a las VLANs	Realizado

Tabla 4-9 Listas de control de acceso

4.5 Seguridad Perimetral

4.5.1 Firewall

La seguridad perimetral es uno de los métodos posibles de defensa de una red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

El espacio protegido, denominado perímetro de seguridad, suele ser propiedad de la misma organización, y la protección se realiza contra una red externa, no confiable, llamada zona de riesgo. Evidentemente la forma de aislamiento más efectiva para cualquier política de seguridad consiste en el aislamiento físico, es decir, no tener conectada la máquina o la subred a otros equipos o a Internet. Sin embargo, en la mayoría de organizaciones los usuarios necesitan compartir información con otras personas, con lo que no es posible un aislamiento total. El punto opuesto consistiría en una conectividad completa con la red, lo que desde el punto de vista de la seguridad es muy problemático. Un término medio entre ambas aproximaciones consiste en implementar cierta separación lógica. De aquí nace la necesidad de lo que hoy día se conoce como cortafuegos.

Figura 4-53 Firewall

Un firewall es un sistema o grupo de sistemas que hace cumplir una política de control de acceso entre dos redes. Puede ser un dispositivo físico o incluso un software sobre un sistema operativo. De una forma más clara, se puede definir un firewall como cualquier sistema utilizado para separar, en lo que a seguridad se refiere, una maquina o subred del resto, protegiéndola así de servicios y protocolos que desde el exterior puedan suponer una amenaza a la seguridad.

La primera pregunta que la empresa puede hacerse es ¿por qué utilizar un firewall? ¿Por qué no configurar simplemente sistemas individuales que hagan frente a los ataques? La respuesta más simple es que el firewall está dedicado a una única cosa: decidir qué comunicaciones son autorizadas y cuáles no. Esto evita la necesidad de tener que comprometer la seguridad, el uso y la funcionalidad.

Sin un firewall, los sistemas se quedan solos con sus propios dispositivos y configuración de seguridad. Estos sistemas pueden estar ejecutando servicios que aumentan la funcionalidad o facilitan la administración, pero no son demasiados seguros y no son de confianza, o solo deberían ser accesibles desde ubicaciones específicas. Los firewalls se utilizan para implementar este nivel de control de acceso.

Si un entorno carece de firewall, la seguridad se basa totalmente en los host. La seguridad será tan fuerte como el host más débil. Cuanto más grande sea la red, más complejo es mantener todos los hosts al mismo nivel de seguridad. Dado que siempre existen descuidos, las intromisiones ocurren debido a errores simples en la configuración y parches de seguridad inadecuados. El firewall es el único punto de contacto con las redes que no son de confianza. Por tanto, en vez de tener que asegurarse de que varias máquinas son lo más seguras posible, el administrador se puede centrar en el firewall, que proporcionará un nivel de protección más frente a un error.

Pero lo que es más, los firewalls son unos auditores excelentes. Como todo el tráfico pasa a través de ellos, la información que contienen sus registros se puede utilizar para reconstruir eventos en caso de una violación de la seguridad.

En general, los firewalls mitigan el riesgo de que los sistemas sean utilizados para propósitos no autorizados o indeseados. Los sistemas y datos corporativos tienen tres riesgos principales contra los que un firewall protege: riesgo de la confidencialidad, riesgo de la integridad de los datos y riesgo de la disponibilidad. Todos estos motivos llevan a las empresas a declinarse por implementar firewalls.

En el capitulo anterior se mostró el diseño físico del firewall de SS.CC, a continuación se muestra el diseño lógico. La entrada a SS.CC. se realiza por el router principal y en caso de fallo por el router de backup. El tráfico se dirige a la IP virtual del firewall, quien filtra los paquetes y solo deja pasar a la red interna o bien a la DMZ (Demilitarized zone) aquellos que no son rechazados.

Una zona desmilitarizada o DMZ es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, es decir, los equipos en la DMZ no pueden conectar con la red interna. Esto permite que los equipos de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los Host situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida. La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera de la red corporativa.

La siguiente figura muestra la estructura de firewall para el IATE.

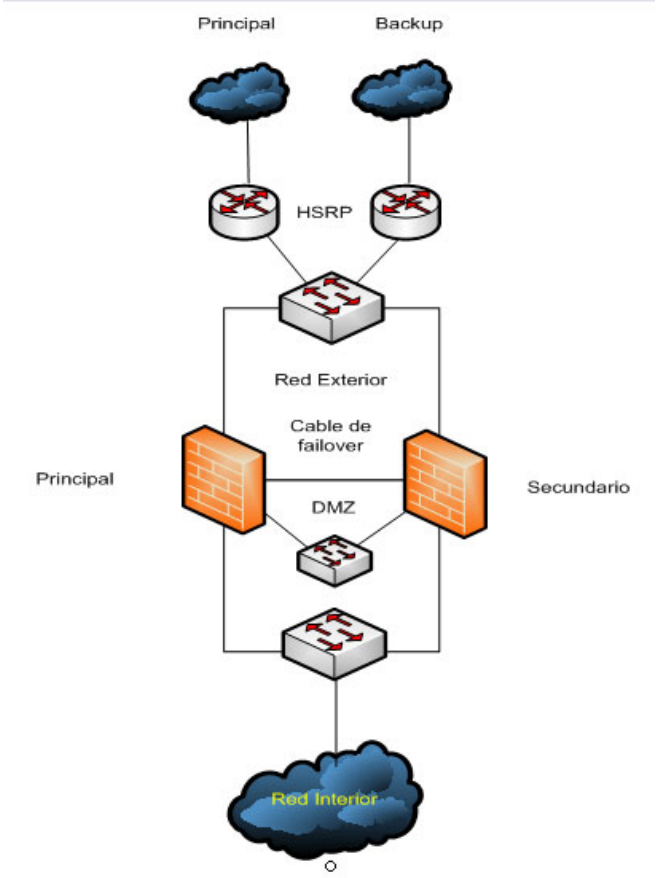


Figura 4-54 Diseño Lógico. Firewall IATE

4.5.2 Iptables y Firewall Builder

El subsistema de red de cualquier sistema operativo actual está diseñado para transmitir, enrutar y recibir tráfico de red. En el caso de los núcleos de Linux, el usuario dispone de una gran cantidad de opciones para procesar los paquetes de la forma más adecuada.

Por filtrado de paquetes se entiende la acción de denegar o permitir el flujo de tramas entre dos redes (por ejemplo la interna, protegida con el firewall, y el resto de Internet) de acuerdo a unas normas predefinidas. En Linux el filtrado de paquetes está programado en el núcleo y se llama Netfilter. Entre las principales características de Netfilter se destacan:

- Filtrado de paquetes
- Traducciones de direcciones de red y puertos
- Manejo avanzado de paquetes

Adicionalmente se dispone de la herramienta Iptables para interactuar con las reglas cuanto se necesite, permitiendo al administrador definir reglas acerca de qué hacer con los paquetes. Estas reglas se agrupan en cadenas, cada cadena es una lista ordenada de reglas. A su vez, las cadenas se agrupan en tablas y cada tabla está asociada con un tipo diferente de procesamiento de paquetes.

Iptables es un sistema de firewall vinculado al núcleo de Linux que se ha extendido enormemente. Está integrado con el núcleo, es parte del sistema operativo, y es una alternativa viable a las extremadamente costosa soluciones de firewall comerciales.

Iptables es una herramienta flexible, potente, gratuita, que funciona sobre un sistema operativo también gratuito, quizás para una organización de I+D o para una empresa no muy grande sea difícil permitirse soluciones comerciales cuyo precio puede ascender a varios millones de pesetas, especialmente si se van a instalar cortafuegos internos o arquitecturas DMZ de varios niveles. Sin embargo, no hay excusa para no utilizar este software de filtrado. Un pequeño PC con Linux es más que suficiente para, en muchas ocasiones, garantizar o al menos incrementar la seguridad de un laboratorio, un aula informática o un conjunto de despachos.

Inicialmente las reglas de filtrado necesarias para poner en marcha el firewall en el IATE son las siguientes:

Origen	Destino	Servicio	Acción	Descripción
VLAN Informativa	**Interfaz eth1**	Cualquiera	Aceptar	Se permite el acceso al Firewall a la VLAN de informática
VLAN Informática	**Cualquiera**	Cualquiera	Aceptar	No se imponen restricciones a la VLAN de informática
Interfaz eth0	**Cualquiera**	http	Aceptar	Se permite la actualización del Firewall
Firewall	**Servidor DNS**	DNS	Aceptar	Acceso al servidor de DNS para la resolución de nombres
Firewall	**Router** **Switch Capa 3** **Switch DMZ**	Ping	Aceptar	Reglas para el Heartbeat
Cualquiera	**Cualquiera**	Hearbeat	Aceptar	Latido
Cualquiera	**Firewall**	Cualquiera	Denegar	Se deniega cualquier tipo de acceso al Firewall
Cualquiera	**DMZ**	http https	Aceptar	Se permite el acceso a la DMZ
VLAN Usuarios	**Cualquiera**	http https	Aceptar	Inicialmente se permite el acceso WEB a los usuarios
VLAN Usuario	**Red Corporativa**	Pop3 Pop3s SMTP Imap Imaps	Aceptar	Se permite el acceso a los servidores de correo de la red corporativa
VLAN Servidores	**Cualquiera**	Cualquiera	Aceptar	No se imponen restricciones a la VLAN de servidores
Servidores DMZ	**BBDD Servidores**	1521 5433 5434	Aceptar	Se permite el acceso desde la DMZ a las BB.DD. de la LAN de servidores
Servidores DMZ	**Servidor DNS**	DNS	Aceptar	Acceso al servidor de DNS para la resolución de nombres
Servidores DMZ	**Servidor NTP**	NTP	Aceptar	Acceso al servidor NTP para la sincronización horaria
Servidores DMZ	**Distinto de las VLANs de:** **Servidores,** **Informática,** **Usuarios**	Cualquiera	Aceptar	Se permite el acceso desde la DMZ a cualquier destino y puerto distinto de las VLAN de informática, servidores y usuarios
Servidores DMZ	**VLANs de:** **Servidores,** **Informática,** **Usuarios**	Cualquiera	Denegar	Se deniega el acceso desde la VLAN de servidores a las VLAN de informática, servidores y usuarios.

Tabla 4-10 Iptables. Reglas de filtrado en el IATE

Por otra parte, Firewall Builder es una herramienta gráfica gratuita muy potente para la configuración y gestión de firewall, que dispone de compiladores de reglas para diversos sistemas de firewall. En la actualidad soporta entre otros Iptables y Cisco. Puede generar ficheros de configuración para cualquiera de estos firewall a partir de una misma configuración, a través de su interfaz grafica, lo que puede ser de gran utilidad en el caso de que se migre de cortafuego.

El uso de esta herramienta no es necesario para poner en marcha el firewall, sin embargo, hay que tener en cuenta que en cuanto se tenga montado un firewall medianamente complejo se tendrá decenas (incluso cientos) de reglas, pudiéndose incluso dar casos de solapamiento entre ellas. Por tanto, su mantenimiento puede ser complicado, y disponer de una herramienta gráfica de esta calidad puede ser vital para controlar el firewall de una forma eficiente y productiva.

En la Figura 4-55 se observan las políticas aplicadas al firewall de SS.CC. En esta misma figura en la parte inferior de la interfaz gráfica existe una zona donde se detallan las características del firewall 1, mientras que en la Figura 4-56 se aprecia el enrutamiento.

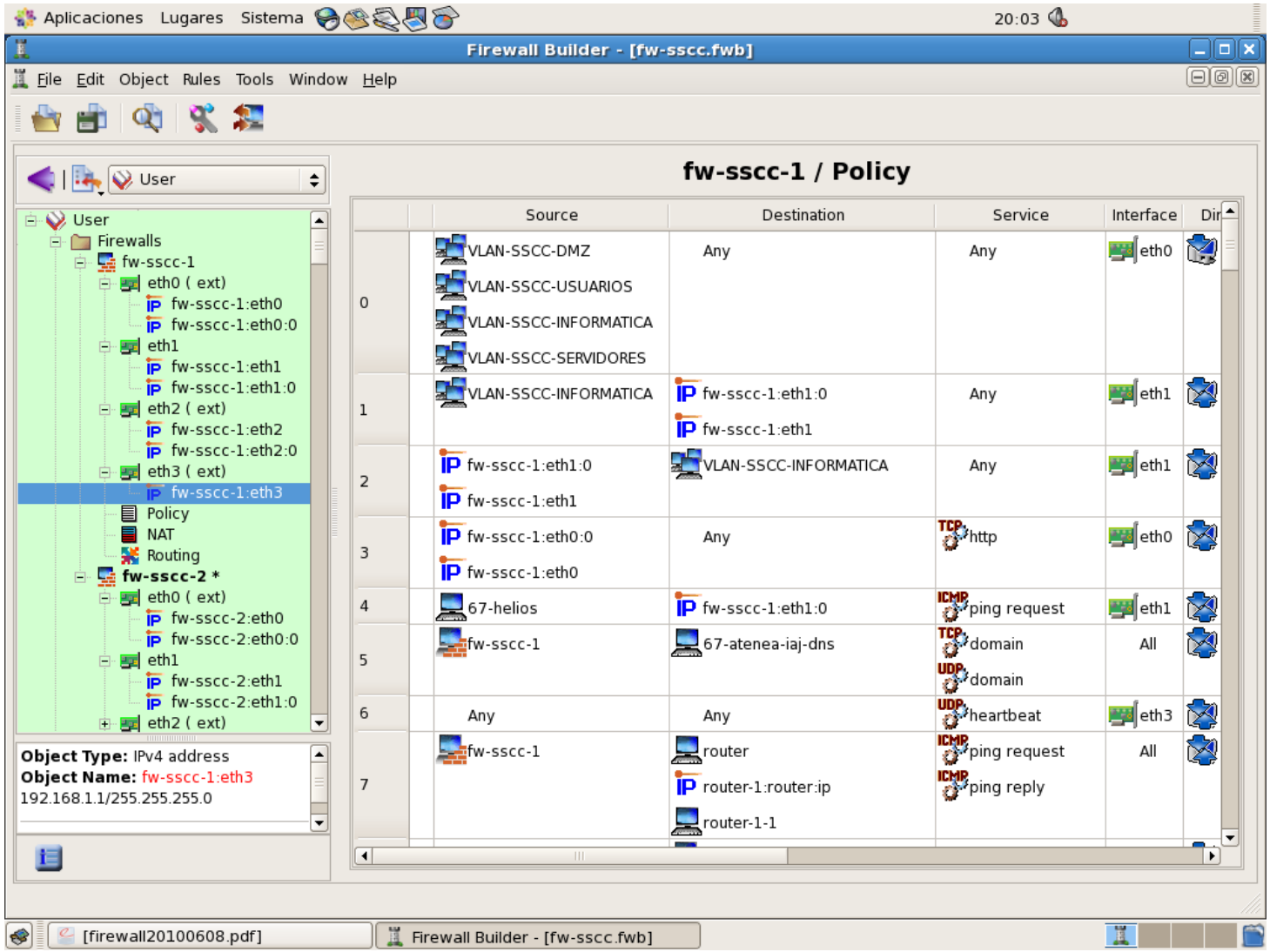


Figura 4-55 Firewall Builder. Policy

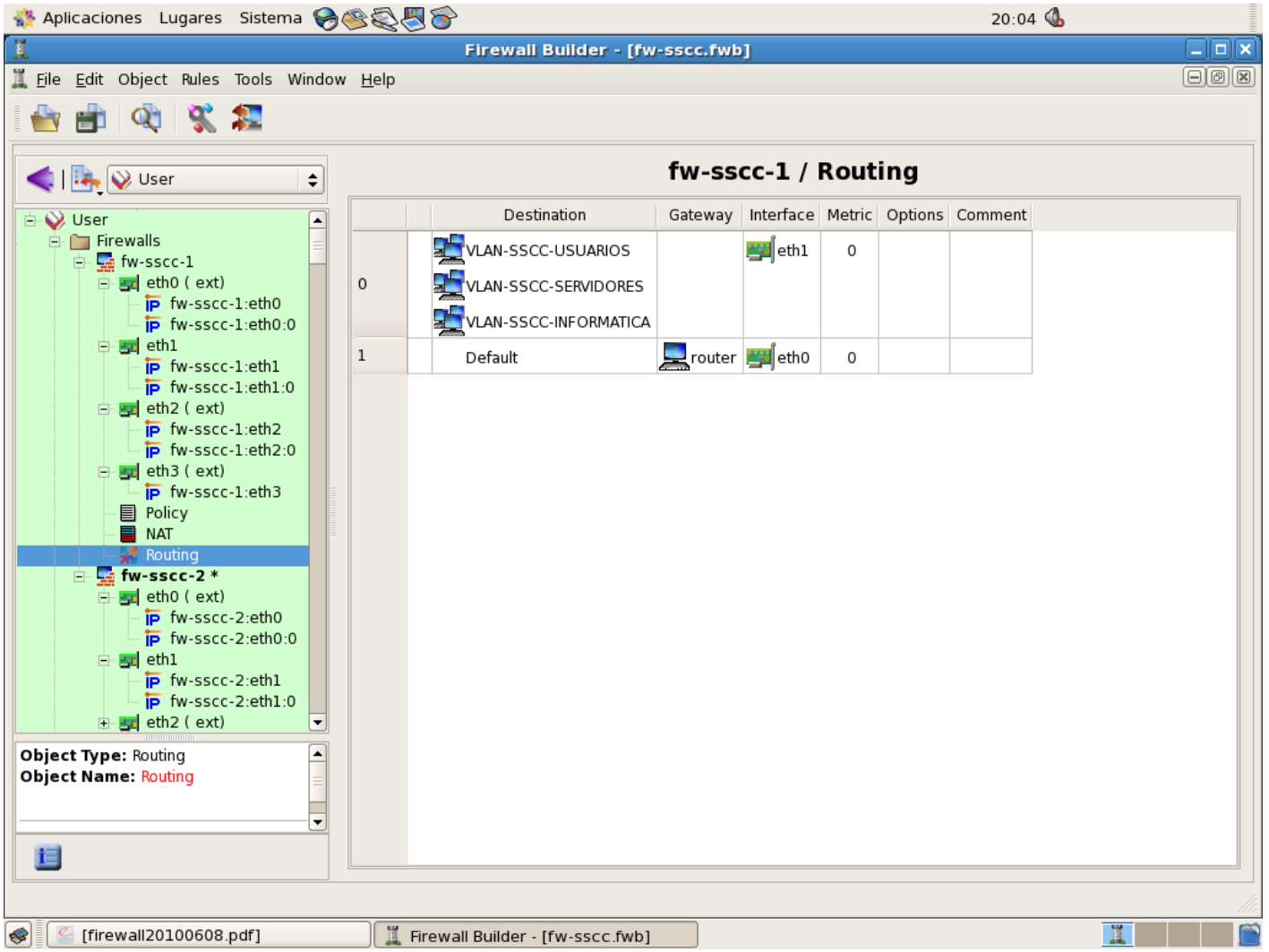


Figura 4-56 Firewall Builder. Routing

4.5.3 Servidores empleados como Firewall

Están ubicados en el CPD del IATE y tienen las siguientes características:

- Fujitsu Siemens Primergy RX220
- 2 x Disco duro 150 Gb
- Raid 1
- 1Gb de RAM
- Procesador 64-bits AMD Opteron 2,2 GHz
- 5 tarjetas de red

4.5.3.1 ¿Que es y que hace heartbeat?

El software heartbeat trabaja enviando latidos (ping), los cuales verifican si el nodo principal está activo o no. Estos pings enviados por heartbeat requieren una respuesta por parte del nodo principal. Si al cabo de un cierto tiempo, el nodo no responde a dichos ping, heartbeat determina que ese nodo se encuentra inactivo o caído, y automáticamente activa el nodo secundario para que asuma el control de la red y los servicios.

4.5.3.2 Paquetes a instalar

Partiendo de una instalación básica de CentOS sólo hay que instalar el paquete heartbeat y sus dependencias:

- ✓ heartbeat-2.1.3-3.el5.centos.i386

4.5.3.3 Ficheros de configuración

/etc/hosts	Se modifica este fichero en las siguientes líneas para indicar las IPs con las que tienen que responder los servidores (cerveros1, cerveros2): 27.0.0.1 cerveros1 localhost.localdomain localhost::1 localhost6.localdomain6 localhost6 192.168.1.1 cerveros1 192.168.1.2 cerveros2
ha.cf	Configuración del log logfacility local0 Debugfile/var/log/ha-debug logfile /var/log/ha-log

	Intervalos entre monitorizaciones keepalive 2
	Tiempo para considerar una maquina muerta deadtime 10
	Tiempo para considerar una maquina muerta tras un reinicio/arranque inicial (debe ser como mínimo el doble que el deadtime) initdead 70
	Puerto UDP para comunicación “ha” entre las maquinas udpport 694
	Interfaz a usar para dicha comunicación bcast eth3
	Configurar que el nodo principal tome el control cuando se levante auto_failback on
	Nombre de la maquinas. Debe coincidir con la salida de uname –n Cerveros1 Cerveros2
	Configurar que en caso de que alguno de los ping sea negativo, pasar el control al de backup ping 10.239.100.1 10.239.101.100 10.239.64.10 respawn hacluster /usr/lib/heartbeat/ipfail apiauth ipfail gid=haclient uid=hacluster
haresources	En este archivo se definen los recursos que son gestionados por HeartBeat. Este fichero debe ser el mismo en ambos nodos. cerveros1 IPaddr::10.239.100.100/24/eth0:0 IPaddr::10.239.101.4/24/eth1:0 IPaddr::10.239.64.1/24/eth2:0 iptables
authkeys	Si el medio es seguro, como por ejemplo una interfaz dedicada para la comunicación entre maquinas "ha", sólo con “crc” para comprobar errores bastará. Si se requiere seguridad “md5” es el idóneo, sin embargo, “sha1” no es muy recomendable, ya que aunque es más seguro consume muchos recursos. Los permisos para el archivo deben de ser 600. auth 1 1 crc
Iptables	Se modifica el start de Iptables start(){ cd /usr/local/bin ; ./fichero-fwbuilder.fw}
/etc/rc.d/rc.local	Con esta ruta se tiene acceso al firewall route add -net 10.239.65.0 netmask 255.255.255.0 dev eth1

Tabla 4-11 Heartbeat. Ficheros de configuración más significativos.

A continuación, la Figura 4-57 ilustra las IPs físicas y virtuales del firewall del IATE, y la Figura 4-58 muestra las interfaces físicas del Firewall activo. La Figura 4-59 y Figura 4-60 muestran el funcionamiento del heartbeat.

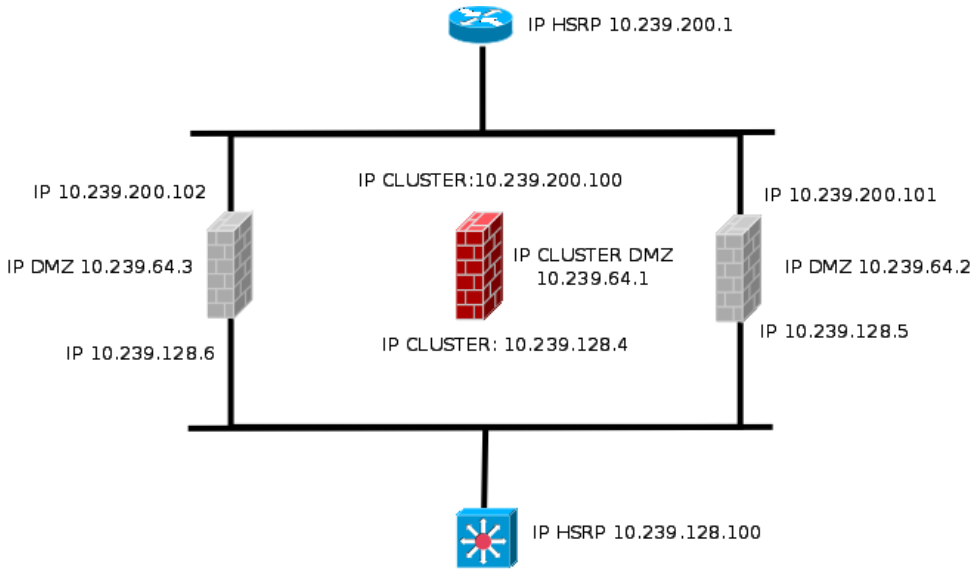


Figura 4-57 Cluster Firewall

```
root@cerveros1:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
eth0      Link encap:Ethernet  HWaddr 00:0A:E4:80:18:46
          inet addr:10.239.200.101  Bcast:10.239.200.255  Mask:255.255.255.0
          inet6 addr: fe80::20a:e4ff:fe80:1846/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1528962199 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2118223359 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2737282090 (2.5 GiB)  TX bytes:2935341770 (2.7 GiB)
          Interrupt:169

eth0:0    Link encap:Ethernet  HWaddr 00:0A:E4:80:18:46
          inet addr:10.239.200.100  Bcast:10.239.200.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:169

eth1      Link encap:Ethernet  HWaddr 00:0A:E4:80:18:47
          inet addr:10.239.128.5  Bcast:20.239.128.255  Mask:255.255.255.0
          inet6 addr: fe80::20a:e4ff:fe80:1847/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2391470674 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2361403425 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3336232068 (3.1 GiB)  TX bytes:2741642820 (2.5 GiB)
          Interrupt:177

eth1:0    Link encap:Ethernet  HWaddr 00:0A:E4:80:18:47
          inet addr:10.239.128.4  Bcast:10.239.128.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:177

eth2      Link encap:Ethernet  HWaddr 00:0E:0C:71:4C:64
          inet addr:10.239.64.5  Bcast:10.239.64.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:cff:fe71:4c64/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2131067278 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1574701899 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1798199939 (1.6 GiB)  TX bytes:3811622692 (3.5 GiB)
          Base address:0x4000 Memory:fc100000-fc120000

eth2:0    Link encap:Ethernet  HWaddr 00:0E:0C:71:4C:64
          inet addr:10.239.64.1  Bcast:10.239.64.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Base address:0x4000 Memory:fc100000-fc120000

eth3      Link encap:Ethernet  HWaddr 00:0E:0C:71:4C:65
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
```

Figura 4-58 Interfaces físicas del Firewall

```
heartbeat[2726]: 2009/09/15_14:53:56 info: Resources being acquired from cervero2.
heartbeat[3135]: 2009/09/15_14:53:56 info: Starting "/usr/lib/heartbeat/ipfail" as uid 498  gid 496 (pid 3135)
harc[3136]: 2009/09/15_14:53:56 info: Running /etc/ha.d/rc.d/status status
mach_down[3191]:  2009/09/15_14:53:57 info: /usr/share/heartbeat/mach_down: nice_failback: foreign resources acquired
IPaddr[3188]:     2009/09/15_14:53:57 INFO:  Resource is stopped
heartbeat[3137]: 2009/09/15_14:53:57 info: Local Resource acquisition completed.
heartbeat[2726]: 2009/09/15_14:53:57 info: mach_down takeover complete.
heartbeat[2726]: 2009/09/15_14:53:57 info: Initial resource acquisition complete (mach_down)
mach_down[3191]:  2009/09/15_14:53:57 info: mach_down takeover complete for node cervero2.
harc[3273]: 2009/09/15_14:53:57 info: Running /etc/ha.d/rc.d/ip-request-resp ip-request-resp
ip-request-resp[3273]:  2009/09/15_14:53:57 received ip-request-resp IPaddr::10.239.100.100/24/eth0:0 OK yes
ResourceManager[3294]:  2009/09/15_14:53:57 info: Acquiring resource group: cervero1 IPaddr::10.239.100.100/24/eth0:0 IPaddr::10.239.101.4/2
IPaddr[3321]:     2009/09/15_14:53:57 INFO:  Resource is stopped
ResourceManager[3294]:  2009/09/15_14:53:57 info: Running /etc/ha.d/resource.d/IPaddr 10.239.100.100/24/eth0:0 start
IPaddr[3419]:     2009/09/15_14:53:57 INFO: Using calculated netmask for 10.239.100.100: 255.255.255.0
IPaddr[3419]:     2009/09/15_14:53:57 INFO: eval ifconfig eth0:0 10.239.100.100 netmask 255.255.255.0 broadcast 10.239.100.255
IPaddr[3390]:     2009/09/15_14:53:57 INFO:  Success
IPaddr[3529]:     2009/09/15_14:53:57 INFO:  Resource is stopped
ResourceManager[3294]:  2009/09/15_14:53:57 info: Running /etc/ha.d/resource.d/IPaddr 10.239.101.4/24/eth1:0 start
IPaddr[3627]:     2009/09/15_14:53:57 INFO: Using calculated netmask for 10.239.101.4: 255.255.255.0
IPaddr[3627]:     2009/09/15_14:53:57 INFO: eval ifconfig eth1:0 10.239.101.4 netmask 255.255.255.0 broadcast 10.239.101.255
IPaddr[3598]:     2009/09/15_14:53:57 INFO:  Success
IPaddr[3736]:     2009/09/15_14:53:58 INFO:  Resource is stopped
ResourceManager[3294]:  2009/09/15_14:53:58 info: Running /etc/ha.d/resource.d/IPaddr 10.239.64.1/24/eth2:0 start
IPaddr[3834]:     2009/09/15_14:53:58 INFO: Using calculated netmask for 10.239.64.1: 255.255.255.0
IPaddr[3834]:     2009/09/15_14:53:58 INFO: eval ifconfig eth2:0 10.239.64.1 netmask 255.255.255.0 broadcast 10.239.64.255
IPaddr[3805]:     2009/09/15_14:53:58 INFO:  Success
ResourceManager[3294]:  2009/09/15_14:53:58 info: Running /etc/init.d/iptables  start
heartbeat[2726]: 2009/09/15_14:54:07 info: Local Resource acquisition completed. (none)
heartbeat[2726]: 2009/09/15_14:54:07 info: local resource transition completed.
heartbeat[2726]: 2009/09/15_14:55:48 info: Link cervero2:eth3 up.
heartbeat[2726]: 2009/09/15_14:55:48 info: Status update for node cervero2: status init
heartbeat[2726]: 2009/09/15_14:55:48 info: Status update for node cervero2: status up
ipfail[3135]: 2009/09/15_14:55:48 info: Link Status update: Link cervero2/eth3 now has status up
ipfail[3135]: 2009/09/15_14:55:48 info: Status update: Node cervero2 now has status init
ipfail[3135]: 2009/09/15_14:55:48 info: Status update: Node cervero2 now has status up
harc[4285]: 2009/09/15_14:55:48 info: Running /etc/ha.d/rc.d/status status
harc[4302]: 2009/09/15_14:55:48 info: Running /etc/ha.d/rc.d/status status
heartbeat[2726]: 2009/09/15_14:55:56 WARN: Late heartbeat: Node cervero2: interval 8000 ms
heartbeat[2726]: 2009/09/15_14:55:57 info: Status update for node cervero2: status active
ipfail[3135]: 2009/09/15_14:55:57 info: Status update: Node cervero2 now has status active
harc[4318]: 2009/09/15_14:55:57 info: Running /etc/ha.d/rc.d/status status
heartbeat[2726]: 2009/09/15_14:55:58 info: remote resource transition completed.
heartbeat[2726]: 2009/09/15_14:55:58 info: cervero1 wants to go standby [foreign]
```

Figura 4-59 Firewall pasivo toma el control

```
heartbeat[2726]: 2009/09/15_14:56:12 info: cervero2 wants to go standby [foreign]
heartbeat[2726]: 2009/09/15_14:56:23 info: standby: acquire [foreign] resources from cervero2
heartbeat[4348]: 2009/09/15_14:56:23 info: acquire local HA resources (standby).
ResourceManager[4361]:  2009/09/15_14:56:23 info: Acquiring resource group: cervero1 IPaddr::10.239.100.100/24/eth0:0 IPaddr::10.239.101.4/2
IPaddr[4388]:     2009/09/15_14:56:23 INFO:  Running OK
IPaddr[4453]:     2009/09/15_14:56:24 INFO:  Running OK
IPaddr[4518]:     2009/09/15_14:56:24 INFO:  Running OK
ResourceManager[4361]:  2009/09/15_14:56:24 info: Running /etc/init.d/iptables  start
heartbeat[4348]: 2009/09/15_14:56:25 info: local HA resource acquisition completed (standby).
heartbeat[2726]: 2009/09/15_14:56:25 info: Standby resource acquisition done [foreign].
heartbeat[2726]: 2009/09/15_14:56:25 info: remote resource transition completed.
heartbeat[2726]: 2009/09/15_15:39:16 info: Heartbeat shutdown in progress. (2726)
heartbeat[5318]: 2009/09/15_15:39:16 info: Giving up all HA resources.
ResourceManager[5331]:  2009/09/15_15:39:16 info: Releasing resource group: cervero1 IPaddr::10.239.100.100/24/eth0:0 IPaddr::10.239.101.4/2
ResourceManager[5331]:  2009/09/15_15:39:16 info: Running /etc/init.d/iptables  stop
ResourceManager[5331]:  2009/09/15_15:39:16 info: Running /etc/ha.d/resource.d/IPaddr 10.239.64.1/24/eth2:0 stop
IPaddr[5696]:     2009/09/15_15:39:16 INFO: ifconfig eth2:0 down
IPaddr[5667]:     2009/09/15_15:39:16 INFO:  Success
ResourceManager[5331]:  2009/09/15_15:39:16 info: Running /etc/ha.d/resource.d/IPaddr 10.239.101.4/24/eth1:0 stop
IPaddr[5776]:     2009/09/15_15:39:16 INFO: ifconfig eth1:0 down
IPaddr[5747]:     2009/09/15_15:39:16 INFO:  Success
ResourceManager[5331]:  2009/09/15_15:39:16 info: Running /etc/ha.d/resource.d/IPaddr 10.239.100.100/24/eth0:0 stop
IPaddr[5856]:     2009/09/15_15:39:17 INFO: ifconfig eth0:0 down
IPaddr[5827]:     2009/09/15_15:39:17 INFO:  Success
heartbeat[5318]: 2009/09/15_15:39:17 info: All HA resources relinquished.
```

Figura 4-60 Firewall activo recupera el control

4.6 Monitorización de la red.

4.6.1 NTop

NTop o Network Top es una plataforma de estadísticas y monitorización de redes, que captura tráfico de forma pasiva y presenta lo que observa en toda una gama de formas. Permite monitorizar en tiempo real los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto y además facilita, a través de flags de colores, la detección de malas configuraciones en algún equipo o servicio.

Otra característica interesante es que implementa su propio servidor WEB, de tal modo que los analistas pueden acceder al estado de la red remotamente desde cualquier navegador.

La configuración del NTOP es bastante sencilla porque utiliza un guión de arranque que configura sus opciones en ejecución.

4.6.1.1 Paquetes a instalar

Toda la paquetería ha sido instalada vía yum install. Los paquetes necesarios son los siguientes:

- ✓ rrdtool-1.4.2-1.el5.rf
- ✓ perl-rrdtool-1.4.2-1.el5.rf
- ✓ ntop-3.3.8-2.el5.rf
- ✓ graphviz-2.22.0-4.el5.rf

4.6.1.2 Ficheros de configuración

El fichero principal de Ntop es ntop.conf situado en el directorio /etc. La siguiente tabla describe los parámetros que se modifican en este fichero.

ntop.conf	Interfaz de red de la que capturar el tráfico --interface eth1
	Por utilizar Puerto SPAN activar la siguiente opción. --no-mac
	Configurar el NTop para generar mensajes de syslog --use-syslog=local3

	-a /var/log/ntop/access.log
	Establecer el puerto usado para http y https --http-server 3000 --https-server 3001
	Establecer las redes que NTop debe considerar locales. --local-subnets 10.239.65.0/24, 10.239.66.0/24, 10.239.67.0/24, 10.239.68.0/24, 10.239.69.0/24, 10.239.70.0/24, 10.239.71.0/24
	Configurar Ntop para que se ejecute como un demonio o servicio del sistema. Lo cual permitirá gestionarlo mediante los clásicos parámetros start, restart, status o stop de cualquier otro servicio. --daemon

Tabla 4-12 NTop. Fichero de configuración más significativo.

4.6.1.3 Interfaz WEB

Para acceder a la interfaz WEB de Ntop, abrir un navegador con la dirección IP del servidor e introducir usuario y contraseña.

http://servidor:3000 o https://servidor:3001

Desde el menú principal, situado en la parte superior, se acceden a las diferentes estadísticas generadas por Ntop.:

Figura 4-61 NTop. Menú de opciones

Los enlaces de mayor interés para el administrador son:

- Summary. Dentro de este menú una de las opciones es “Network Load”, que muestra estadísticas de la carga de red durante los últimos 10 minutos, la ultima hora, el día actual e incluso del mes completo. La siguiente figura demuestra que el tráfico en el IATE durante los últimos diez minutos y en la última hora (del día en el cual se han tomando las capturas) es normal, ya que de los 20Mbps disponibles se observa que por regla general se están utilizando menos de 2Mbps.

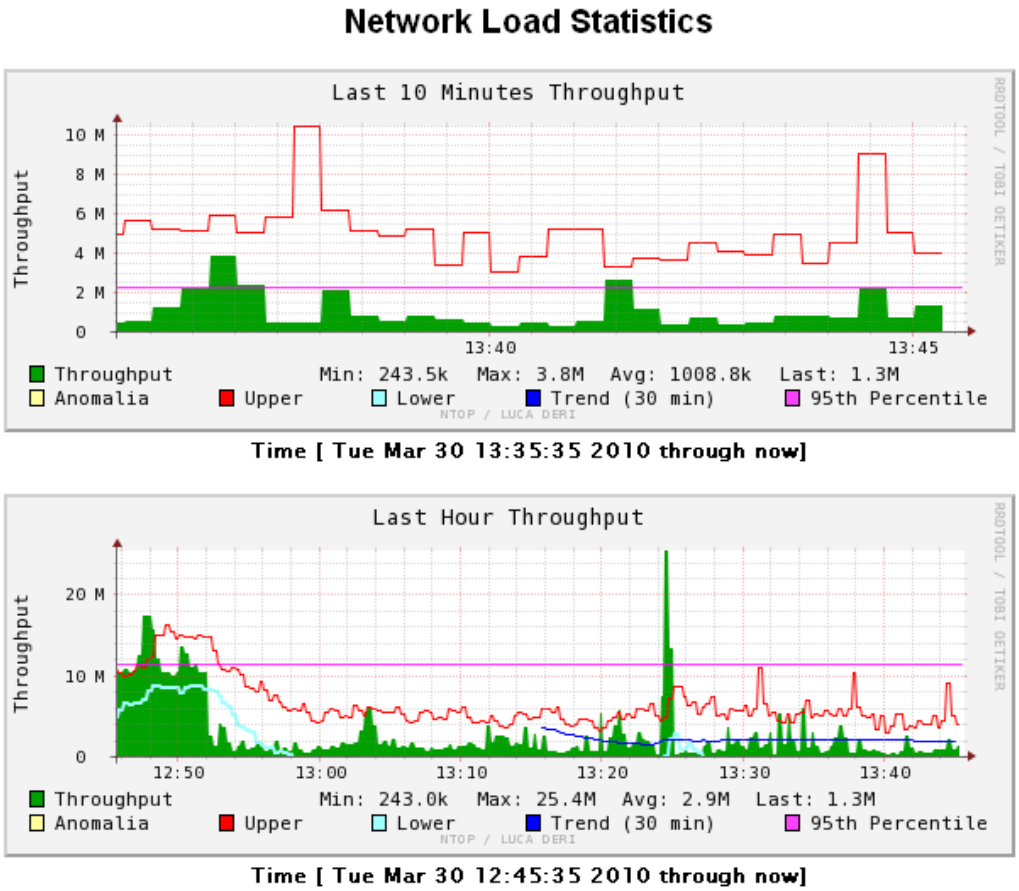


Figura 4-62 NTop. Summary. Network Load

Otra de las opciones dentro de Summary es “Traffic”, que permite acceder a la visión global del trafico generado en la red, a la distribución por protocolo, la carga de la red y otros datos de interés.

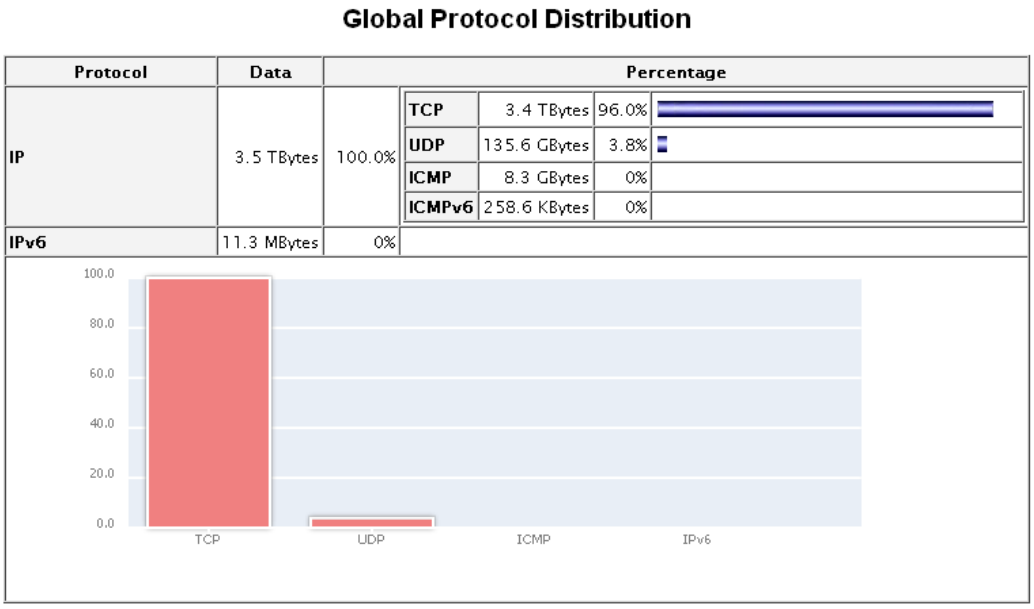


Figura 4-63 NTop. Summary. Resumen de distribución por protocolo

- All protocols. Dentro de este menú se encuentra también otra opción denominada "Traffic", que muestra las direcciones IP vistas por NTOP y los servicios que han utilizado. En este mismo menú existe la opción "Throughput", que permite ver el tráfico generado en la red por cada Host en el instante actual.

Network Throughput: All Hosts - Data Sent+Received

Hosts: All Data: All

Host	Domain	Data			Packets		
		Current	Avg	Peak	Current	Avg	Peak
10.239.66.158		3.0 Mbit/s	10.0 bit/s	3.0 Mbit/s	280.7 Pkt/s	0.0 Pkt/s	280.7 Pkt/s
mail.		3.0 Mbit/s	10.0 bit/s	3.0 Mbit/s	280.7 Pkt/s	0.0 Pkt/s	280.7 Pkt/s
desdeelcielo		495.3 Kbit/s	20.4 bit/s	1.0 Mbit/s	53.1 Pkt/s	0.0 Pkt/s	114.7 Pkt/s
10.239.66.117		495.3 Kbit/s	30.2 bit/s	1.0 Mbit/s	53.1 Pkt/s	0.0 Pkt/s	114.7 Pkt/s
proxy.		323.0 Kbit/s	157.5 bit/s	3.6 Mbit/s	61.0 Pkt/s	0.0 Pkt/s	672.7 Pkt/s
-antivirus		143.9 Kbit/s	134.4 Kbit/s	41.1 Mbit/s	15.0 Pkt/s	11.8 Pkt/s	3673.6 Pkt/s
10.143.64.127		112.4 Kbit/s	0.3 bit/s	112.4 Kbit/s	10.9 Pkt/s	0.0 Pkt/s	10.9 Pkt/s
www.iaap		76.9 Kbit/s	0.7 bit/s	147.4 Kbit/s	7.4 Pkt/s	0.0 Pkt/s	15.4 Pkt/s
neptuno.		57.4 Kbit/s	1.6 Kbit/s	4.9 Mbit/s	17.2 Pkt/s	0.4 Pkt/s	1036.6 Pkt/s

Figura 4-64 NTop. All Protocols. Network Throughput

De la figura anterior se desprende que el equipo "10.239.66.158" está enviando un correo de 3Mbps, que además coincide con el host "mail"

- IP. Da información acerca del sentido del tráfico, si va de la red local a una red remota, o viceversa, además de estadística de uso a nivel de red, es decir, como conjunto de Hosts.

IP Protocol	Data	Percentage
TCP vs. UDP	781.9 GBytes	TCP 99.0 % / UDP 1.0 %

TCP/UDP Protocol	Data	Percentage
FTP	75.2 GBytes	9.6%
HTTP	568.3 GBytes	72.7%
DNS	2.5 GBytes	0%
Telnet	182.8 MBytes	0%
NBios-IP	1.9 GBytes	0%
Mail	93.0 GBytes	11.9%
SNMP	259.6 MBytes	0%
NFS/AFS	3.8 GBytes	0%
VoIP	4.9 MBytes	0%
X11	5.5 KBytes	0%
SSH	34.6 GBytes	4.4%
Gnutella	0.8 KBytes	0%
Kazaa	29.7 MBytes	0%
WinMX	0.2 KBytes	0%
eDonkey	1.1 GBytes	0%
BitTorrent	38.4 KBytes	0%
Messenger	1.1 GBytes	0%
Other TCP/UDP-based Protocols	49.2 MBytes	0%

Figura 4-65 NTop. Distribución por protocolo

De la Figura 4-65 se deduce que el mayor porcentaje de tráfico es http y seguidamente en menor medida Mail.

- Plugins. Permite añadir plugins a NTop para ampliar sus funcionalidades.
- Admin. Permite modificar las opciones de configuración de Ntop, así como cambiar la interfaz de red y el mantenimiento de usuarios, entre otras.

4.6.2 ARPWatch

En sistemas Linux esta herramienta puede servir para detectar el uso del envenenamiento ARP. Con ARPWatch se puede comprobar la correspondencia entre parejas de direcciones IP-MAC (Ethernet). En el caso de que se produzca un cambio en un par, ARPWatch envía un correo de notificación del suceso al administrador del sistema. También permite monitorizar la existencia de nuevos hosts al detectar la aparición de una nueva MAC en la red. De este modo, el asunto de los correos enviados comunica uno de los siguientes avisos:

- New Station. Se ha detectado un nuevo par MAC/IP
- New Activity. El par MAC/IP, que ya estaba registrado, vuelve a tener actividad después de seis meses o más sin uso.
- Changed Ethernet Address. Se ha detectado que la dirección IP ha cambiado a una nueva dirección MAC. Esto puede ser indicio de un ataque y debe ser comprobado.
- Flip Flop. Se ha detectado que la dirección MAC ha cambiado desde el último valor registrado al penúltimo. Puede ser un indicio de ataque y debe ser comprobado.

4.6.2.1 Paquetes a instalar

Toda la paquetería ha sido instalada vía yum install. Los paquetes necesarios son los siguientes:

- ✓ libcap-1.10-26
- ✓ arpwatch-2.1a13-21.el5

4.6.2.2 Ficheros de configuración

La Tabla 4-13 destaca los ficheros de configuración más relevantes para el ARPWatch.

arpwatch	Es el fichero principal de ARPWatch y está situado en /etc/sysconfig/arpwatch. Su contenido es similar al siguiente: OPTIONS="-u pcap -n RED/MASCARA -e correo@uca.es -s 'root (Arpwatch)'" Las opciones más utilizadas son: -n: Red que se va a monitorizar -e: Correo electrónico en el cual se desea recibir las alarmas
arp.dat	Situado en /var/arpwatch/arp.dat. Mantiene una base de datos con la estructura MAC/IP. Los mensajes descritos anteriormente avisan de cambios producidos en este fichero.

Tabla 4-13 ARPWatch. Ficheros de configuración más significativos.

4.6.2.3 Sonda ARPWatch

Para el IATE se han adquirido equipos cuya finalidad es funcionar como sondas en cada uno de los segmentos de los usuarios, es decir, en las VLANs de Muñoz Olivé, Bilbao y O'Donell. Estos equipos están situados dentro del CPD del SS.CC., conectados en el switch ScSwitch05, como se puede observar en la Figura 4-66. Sus características son las siguientes.

- Fujistsu Siemmes p300
- Procesador: Intel® Pentium® 4 2400 MHz
- Memoria: 512MB DDR 400
- Disco Duro: 20 GB Ide Ultra ATA
- Tarjeta de Red: 10/100 MB.

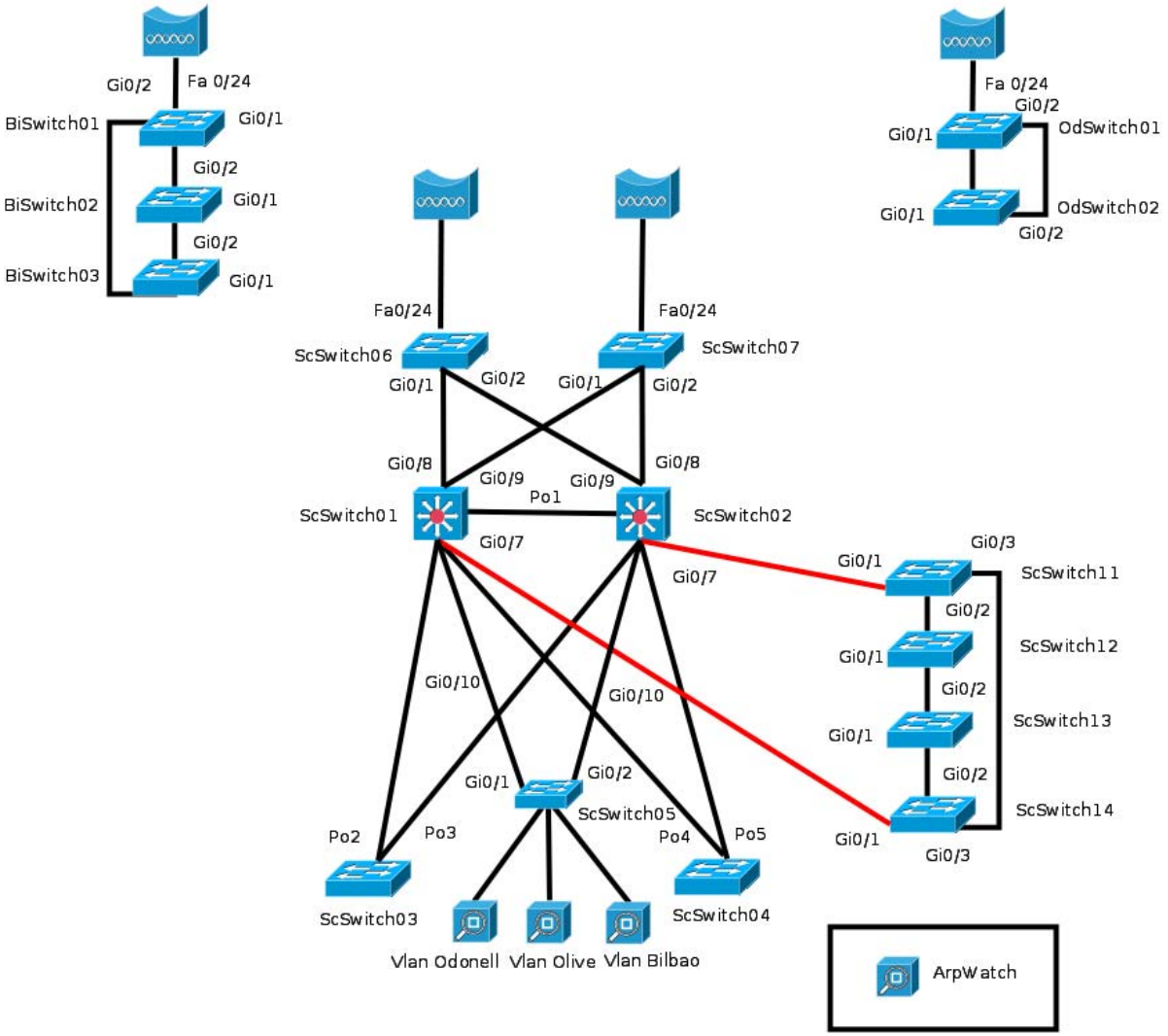


Figura 4-66 Sonda ARPWatch

4.7 Conclusiones

Las amenazas a la seguridad de la información atentan contra su confidencialidad, integridad y disponibilidad. Existen amenazas relacionadas con fallos humanos y otras con ataques malintencionados. Mediante la materialización de una amenaza podría ocurrir el acceso, modificación o eliminación de información no autorizada, la interrupción de un servicio o incluso daños físicos en el equipamiento. De ahí la importancia de implementar buenas medidas de seguridad que protejan a la organización de estos ataques.

A lo largo del capítulo se han explicado en detalle los ataques más comunes que atentan contra los dispositivos de capa 2, agrupados en tres categorías: Ataques de capa MAC, ataques VLAN y ataques por sustitución o spoofing. De este modo, se han estudiado amenazas tales como MAC Flooding, VLAN Hopping en sus dos variantes, ataques STP o Spoofing de DHCP, MAC, y ARP.

Con el fin de mantener rigor en la exposición, en cada uno de los respectivos apartados se ha descrito la forma de llevar a cabo dicho ataque y seguidamente se han tratado los métodos o estrategias para mitigarlo. En ese sentido, resaltar que los switches de Cisco ofrecen características para la configuración de seguridad en puerto que son de gran ayuda.

Los estudios documentados en el capitulo 2, sacaron a relucir que la red actual del IATE no implementa ningún mecanismo de seguridad, de manera que cualquier usuario fácilmente puede pinchar su equipo en la red y obtener una dirección IP. Debido a esto, se suelen producir ataques MAC Flooding, DHCP Spoofing, MAC Spoofing y ARP Spoofing, que ponen en peligro la integridad y disponibilidad de la red.

Pero además en el capitulo anterior se contempló la creación de VLANs, y el uso del protocolo STP para tratar la redundancia en capa 2. Mejoras que a su vez pueden conducir a la aparición de amenazas del tipo VLAN Hopping y ataques STP.

Uno de los puntos más importante de esta sección es el de enfoques básicos para la protección de switches de capa 2, puesto que recoge todas las medidas orientadas a la seguridad en la LAN que se van a aplicar en el IATE durante el desarrollo de este proyecto fin de carrera. Ente las que se destacan además de la configuración de seguridad en puerto, configuración de los puertos del switch en modo acceso, deshabilitar DTP en todos los puertos que no necesiten formar un enlace troncal, no enviar datos de usuario sobre una VLAN nativa, utilizar mecanismos de protección STP y habilitar DHCP Snooping.

También se ha estudiado el tema de las listas de control de acceso en sus diferentes tipos, como medida de seguridad con el fin de filtrar o comprobar paquetes, y determinar así si deben reenviarse a su destino o descartarse.

Por ultimo, se ha tratado la seguridad perimetral, ya que con el acceso a Internet la red de datos se ve expuesta a ataques y accesos no autorizados por parte de usuarios externos e internos. El Firewall separa una maquina o subred del resto, protegiéndola así de servicios y protocolos que desde el exterior puedan suponer una amenaza a la seguridad, mediante la imposición de políticas de seguridad en el acceso a los recursos de la red y hacia la red externa. Como ejemplo de implementación software de un firewall vinculado al sistema operativo Linux se ha considerado el filtrado por Iptables, alternativa bastante flexible y enormemente extendida.

Finalmente, se han descrito las herramientas Firewall Builder, NTop y ARPWatch. La primera de ellas permite controlar el firewall de forma eficiente, mientras que las otras dos se utilizan para monitorizar la red. NTop se ha presentado como una excelente herramienta de software libre para conocer a fondo la utilización del canal, y la información que presenta sirve además para optimizar el firewall, ya que permite detectar tráfico en puertos o en máquinas en las cuales no debería haberlo o detectar abusos por parte de usuarios que indiscriminadamente utilizan todo el ancho de banda disponible.

Capítulo 5.
Diseño de la WLAN

5.1 Introducción

El diseño de la red del IATE culmina con un capítulo dedicado al diseño de la WLAN externa (Wireless LAN), cuya función principal es dotar de cobertura inalámbrica, como extensión de la LAN, a las oficinas de Muñoz Olivé, Bilbao y O'Donell. Esto permite unir a los tres edificios que constituyen los SS.CC. del IATE, conectados hasta el momento a través de una línea LAN to LAN, mediante un enlace de red inalámbrica con la máxima seguridad disponible.

El proceso seguido para el diseño de la WLAN se puede dividir en las fases mostradas en la figura.

Figura 5-1 Fases del diseño de la WLAN

Las tres fases intermedias, estudio de la cobertura, adquisición del equipamiento y prueba piloto, han sido llevadas a cabo por una empresa externa, encargada de la instalación de las antenas externas en los tres edificios. En un principio, y antes de la instalación final, la empresa externa ha realizado una prueba de cobertura, con la idea de certificar el correcto estado del enlace. Para completar el proceso, en el presente proyecto fin de carrera se cubren las fases 1, 5 y 6, diseño lógico, despliegue de la red, y actualización de la documentación de la red (Anexo C) para incorporar los cambios derivados del diseño de la WLAN externa.

5.2 Diseño de la Wireless externa

5.2.1 FASE 1. Arquitectura lógica y física de la WLAN

Como se comentó en el capitulo 2, las sedes Muñoz Olivé, O'Donell y Bilbao se comunican con líneas LAN to LAN, cuyo alquiler supone un desembolso mensual para el IATE.

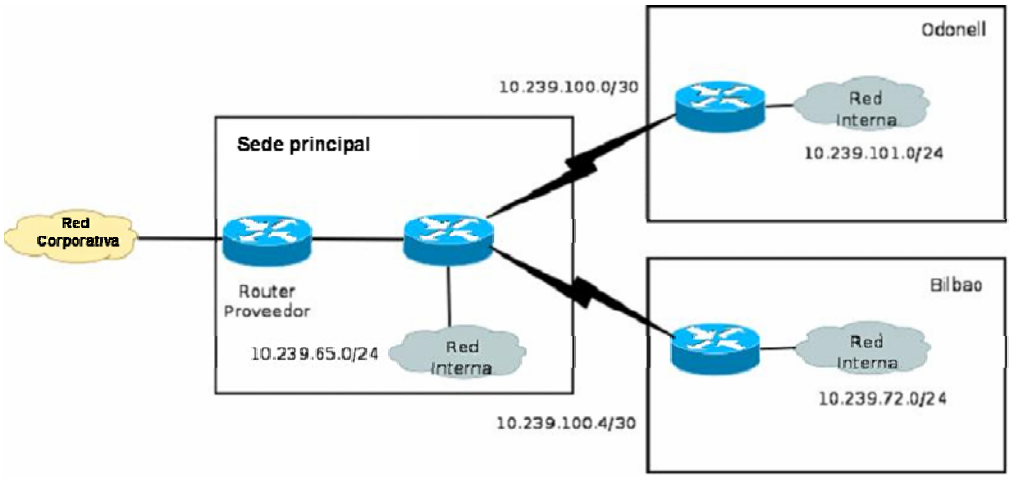


Figura 5-2 Diseño Lógico basado en línea LAN to LAN

Con objeto de reducir gastos se ha decidido implantar radio enlaces para unir estos edificios. Para desarrollar esta solución se van a instalar en Muñoz Olivé dos puentes inalámbricos, uno apuntando a la sede de O'Donell y otro orientado hacia la sede de Bilbao. Al incluir la WLAN externa en el diseño lógico de la red del IATE, los edificios de Bilbao y O'Donell van a ocupar las VLAN 5 y 6, respectivamente.

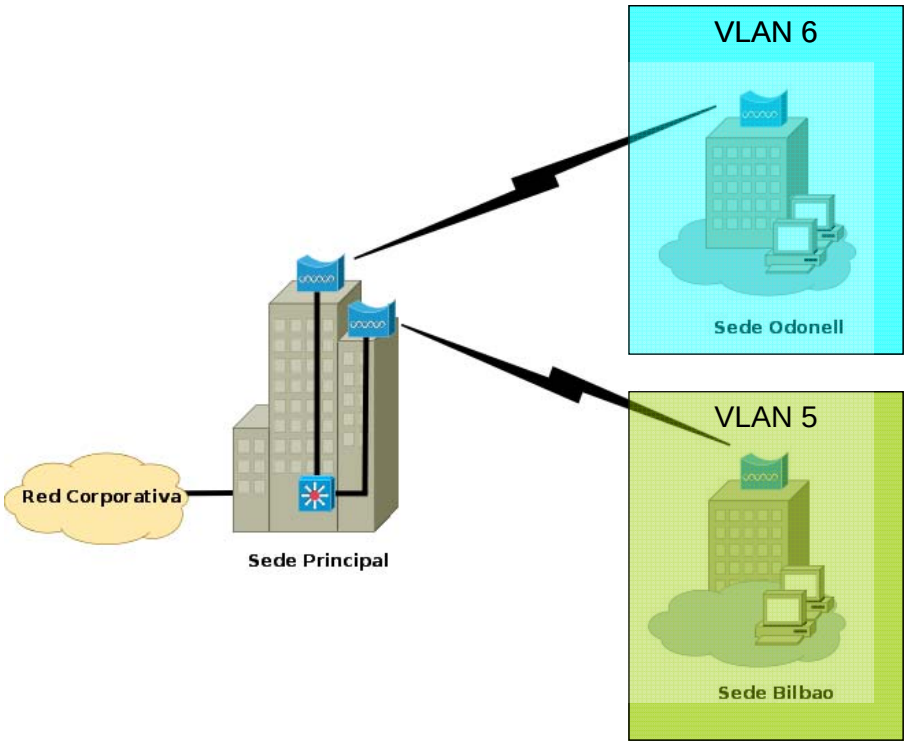


Figura 5-3 Diseño Lógico basado en WLAN

La arquitectura Física de la red del IATE ya se estudió en el capítulo 3. Como se puede observar, en ella se incluye también la arquitectura Física correspondiente a la WLAN externa.

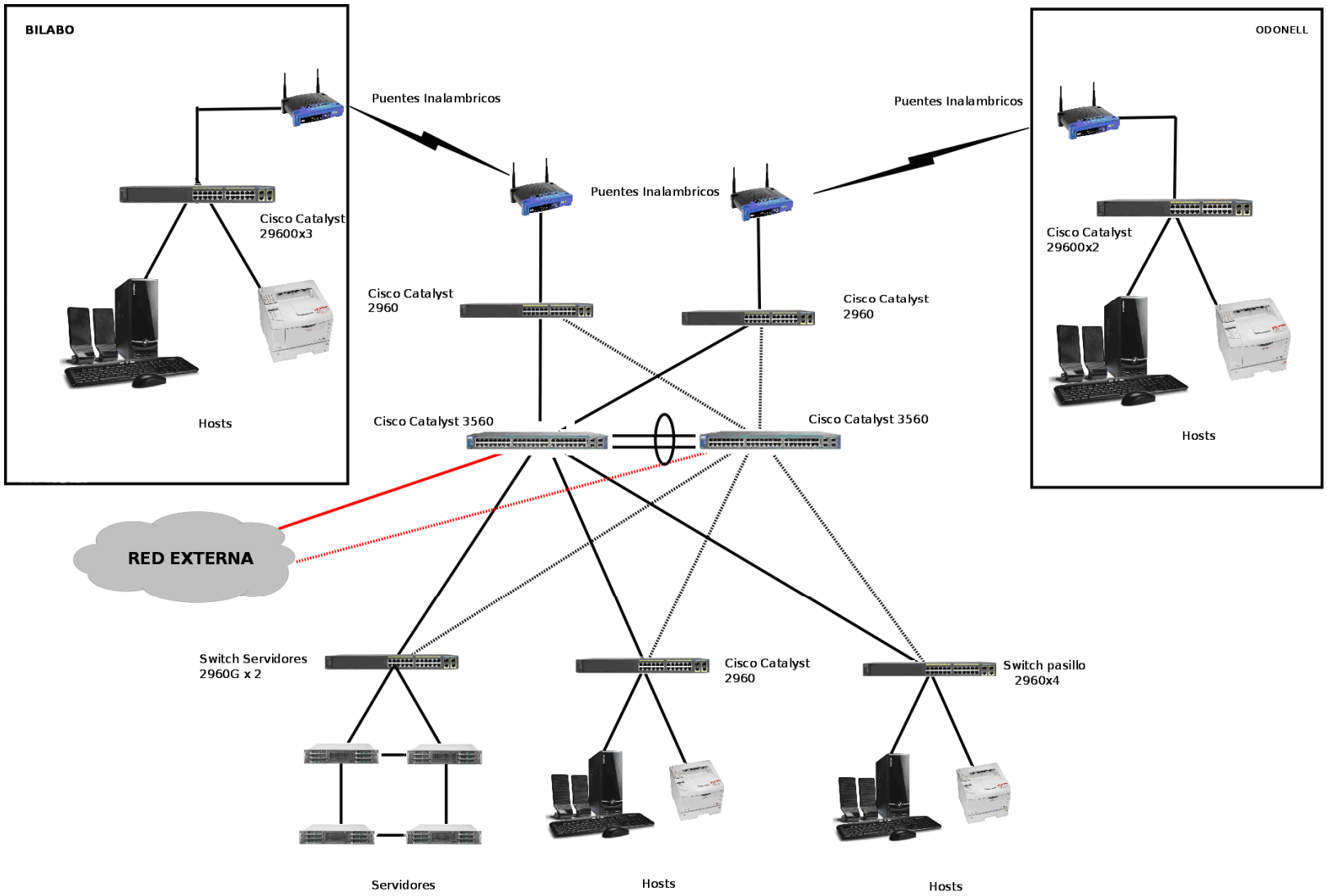


Figura 5-4 Arquitectura Física para la WLAN

5.2.2 FASE 2. Estudio de cobertura

Las especificaciones de la red cubren aspectos relativos a la cobertura radioeléctrica y accesibilidad. Todo este estudio ha sido contratado, como se ha indicado anteriormente, a una empresa externa. Aquí se recogen las conclusiones más relevantes a modo de resumen.

- Cobertura radioeléctrica. Los edificios se han enlazado con un nivel de señal suficiente para alcanzar los 54 Mbps de capacidad de pico y de tal modo que la relación señal/ruido nunca sea inferior a SNR 20db, asegurando la estabilidad de los enlaces.

- Accesibilidad. El acceso por parte de los usuarios al otro extremo del radio enlace es transparente.

Se han tenido en cuenta las siguientes consideraciones relativas al rendimiento:

- Con el fin de mejorar el rendimiento de los puentes, se ha limitado la asociación a clientes 802.11g (OFDM), no permitiéndose redes mixtas 802.11b.
- La configuración del canal radio se establece automáticamente entre los canales 1 a 13.
- Las antenas conectadas a los puentes son especiales para exterior.
- Los puentes controlan la potencia de transmisión vía software.

Se han tenido en cuenta las siguientes consideraciones relativas a la seguridad física y lógica del diseño elegido.

- El SSID (Service Set Identifier) elegido para cada edificio no guarda relación directa con el IATE y se deshabilitará su difusión.
- Los logs se pueden redireccionar a un servidor de Syslog.
- En los puentes se ha deshabilitado DHCP.
- El cifrado es del tipo WPA2 (Wifi Protected Access 2)
- Autentificación mediante contraseña en los puentes (WPA2 personal para bridge).
- Rotación de claves de intercambio entre los puentes.

5.2.3 FASES 3 y 4. Adquisición del equipamiento y prueba piloto.

Como ya se comentó en el capítulo 3, el equipamiento adquirido para el despliegue de la WLAN externa han sido 4 puentes inalámbricos del tipo Bridge Linksys modelo WAP54G. Para una información más detallada sobre estos dispositivos, se adjuntan las especificaciones de los mismos en el anexo B, Hardware Empleado.

La adquisición del material necesario para la puesta en marcha de la red inalámbrica entre los edificios Muñoz Olivé, Bilbao y O'Donell ha sido responsabilidad de una empresa externa, por lo tanto, no es objeto de este proyecto. Sin embargo, comentar que la elección se ha basado fundamentalmente en el aspecto económico, el cliente dejó claro de antemano que su deseo era únicamente sustituir una conexión LAN to LAN de alquiler por un enlace inalámbrico, sin mayores ambiciones que las de reducir costes y tratando de evitar una inversión inicial demasiado elevada.

Antes de la entrega del equipamiento, la empresa externa responsable ha certificado el correcto funcionamiento de la infraestructura proporcionada mediante una prueba piloto de cobertura, realizada en dos etapas, primero con uno solo de los nodos del equipamiento final, y posteriormente con ambos nodos. Finalmente, también han realizado algunas pruebas reales de caídas y otros fallos.

5.2.4 FASE 5. Despliegue

La configuración de los puentes inalámbricos se ha realizado durante el desarrollo del presente proyecto fin de carrera, pero se tratará junto con la configuración de la electrónica de red. Tras configurar todos los equipos, será entonces cuando se podrá poner en marcha la red completa del IATE y realizar las pruebas pertinentes. Todo esto se irá viendo en los próximos capítulos.

5.2.5 FASE 6. Documentación de la red

Al igual que el resto de equipos, la información necesaria sobre los puentes inalámbricos ha sido incorporada a la documentación de la red (Ver Anexo C).

Puente inalámbrico	IP	Mascara	Estática/Dinámica	VLAN
Puente SSCC-Bilbao	10.239.68.253	255.255.255.0	Estática	VLAN 5
Puente SSCC-O'Donell	10.239.69.253	255.255.255.0	Estática	VLAN 6
Puente Bilbao	10.239.68.254	255.255.255.0	Estática	VLAN 5
Puente O'Donell	10.239.69.254	255.255.255.0	Estática	VLAN 6

Tabla 5- 1 Documentación de la red inalámbrica

5.3 Conclusiones

Las redes inalámbricas de área local (WLAN) son una realidad hoy en día y están teniendo un gran éxito en el mercado, gracias a que sus precios han disminuido considerablemente. Existe todo un abanico de productos y sistemas que permiten desplegar redes inalámbricas fiables y asequibles en precio y prestaciones.

La tecnología WIFI, cómo se le conoce comúnmente a las WLANs, utiliza frecuencias de radio (RF) para transmitir información, en vez de utilizar los tradicionales cables para comunicación. Es relativamente fácil crear una red híbrida, que permita seguir teniendo las ventajas de la velocidad que brinda la parte cableada y expanda las posibilidades con la parte inalámbrica.

La aplicación de la tecnología WIFI a este proyecto fin de carrera ha tenido una finalidad muy concreta, unir mediante red inalámbrica los tres edificios que constituyen los SS.CC. del IATE, persiguiendo reducir los costes que suponía el alquiler de la línea LAN to LAN empleada hasta el momento para este fin.

La planeación y el diseño de una red, por pequeña que se ésta, permite sacarle un mayor provecho, logrando un mejor desempeño en términos de velocidad de transmisión, así como reducir el nivel de inseguridad que presentan este tipo de redes. Parte de este proceso ha sido contratado a una empresa externa, responsable de inspeccionar el terreno, realizar los estudios de cobertura y seleccionar los equipos. Durante el desarrollo de este proyecto, se ha colaborado en dicho proceso planteando el diseño lógico de la red, realizando actividades de seguimiento y control de los trabajos sub-contratados, actualizando la documentación de la red para incorporar la asignación de direcciones IPs dada a los dispositivos inalámbricos, y como se verá en próximos capítulos, configurando los puentes inalámbricos y llevando a cabo la puesta en marcha de la red completa.

Capítulo 6.
Configuración

6.1 Introducción

Tras haber finalizar el diseño de la VLAN, ha llegado el momento de proceder a la configuración de la electrónica de red Cisco para que cumpla con las decisiones de diseño expuestas en capítulos anteriores.

Este capítulo comienza detallando los comandos necesarios para la configuración de parámetros básicos y comunes para cualquier tipo de switch, tales como contraseñas, nombre del host, IP de administración y Gateway por defecto. Del mismo modo, se toma como ejemplo un switch de capa 2 para tratar temas como la configuración de VLAN, de las medidas de seguridad, y la redundancia en capa 2 mediante STP, entre otros.

A continuación, se dedica un apartado a la configuración de características específicas de un switch de capa 3, entre las que se incluyen habilitar las funciones de enrutamiento, creación del dominio VTP, configuración del puente raíz y de los puertos enrutados, configuración de la redundancia en capa 3 mediante HSRP, configuración de listas de control de acceso del tipo RACL y VACL, configuración del DHCP y de las interfaces.

Finalmente, se exponen los pasos necesarios para configurar los puentes inalámbricos, necesarios para el despliegue de la WLAN.

6.2 Configuración del Switch

Lo descrito en este apartado es de aplicación para cualquier tipo de switch, ya sea de capa 2 o 3. Durante el desarrollo del presente proyecto fin de carrera se ha llevado a cabo la configuración de cada uno de los switches pertenecientes a la red del IATE. Aunque para la elaboración de este apartado se haya elegido el switch de capa 2, ScSwitch12, que se encuentra en Muñoz Olivé, el proceso de configuración de estos parámetro en cada uno de los switches es análogo y consistiría en repetir los mismos pasos para cada uno de ellos.

6.2.1 Configuración de fábrica por defecto.

El inicio de un switch Catalyst requiere la ejecución de los siguientes pasos:

- **Paso 1**. Antes de poner en funcionamiento el switch, es necesario verificar que todos los cables de red están correctamente conectados y que el equipo está conectado al puerto de consola. La Figura 6-1 ilustra cómo conectar una PC a un switch mediante el puerto de consola.

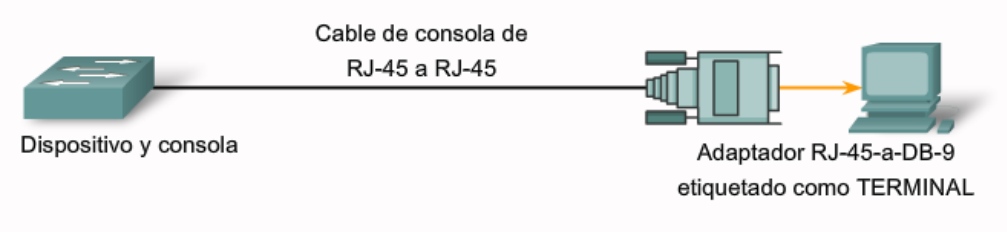


Figura 6-1 Conexión del Switch a un PC

Por otra parte, hay que ejecutar la aplicación del emulador de terminal conocida como HyperTerminal, y asegurarse que ésta esté correctamente configurada. Esta aplicación se utiliza para ver la consola de un dispositivo Cisco. La Figura 6-2 muestra la correcta configuración del HyperTerminal.

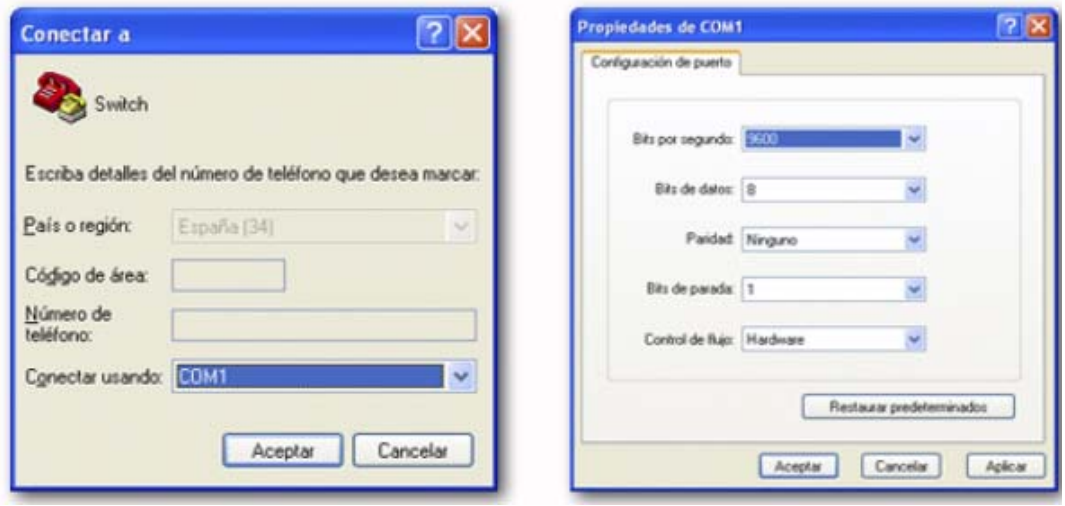


Figura 6-2 Configuración del HyperTerminal

- **Paso 2**. Conectar el cable de alimentación. El switch se pondrá en funcionamiento. Algunos switches Catalyst, incluida la serie Cisco Catalyst 2960, no disponen de botón de encendido.

- **Paso 3**. Observar que la secuencia de arranque transcurra adecuadamente. Al encender el switch, éste inicia una prueba denominada POST. Durante la POST, los indicadores de los LED parpadean mientras una serie de pruebas internas determinan si el switch está funcionando correctamente. Cuando la POST finaliza con éxito, el LED SYST pasa a tomar

el color verde. Si el switch no pasa la prueba POST, el LED SYST se pone de color ámbar, y en tal caso, será necesario repararlo.

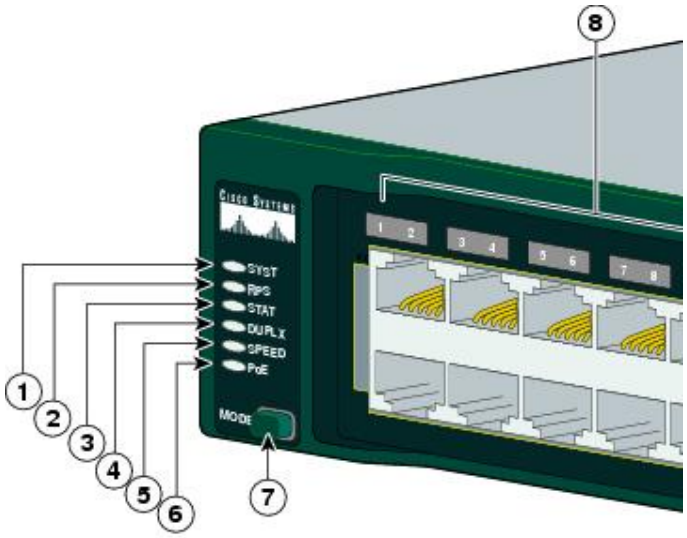


Figura 6-3 Indicadores LEDs del switch

En la figura anterior, el LED SYST ocupa la posición 1. La Tabla 6-1 resume los estados que este led puede tomar y su significado.

Apagado		El sistema no recibe corriente
Color	**Verde**	El sistema funciona correctamente
	Ámbar	El sistema esta recibiendo energía pero no funciona correctamente.

Tabla 6-1 Estados del LED SYST del switch

La Figura 6-4 muestra la salida por consola del proceso de arranque. Una información similar se puede obtener mediante el uso del comando show post, como puede verse en la Figura 6-5.

```
Initializing flashfs...

flashfs[1]: 363 files, 5 directories
flashfs[1]: 0 orphaned files, 0 orphaned directories
flashfs[1]: Total bytes: 32514048
flashfs[1]: Bytes used: 11160064
flashfs[1]: Bytes available: 21353984
flashfs[1]: flashfs fsck took 1 seconds.
flashfs[1]: Initialization complete....done Initializing flashfs.

POST: CPU MIC register Tests : Begin
POST: CPU MIC register Tests : End, Status Passed

POST: PortASIC Memory Tests : Begin
POST: PortASIC Memory Tests : End, Status Passed

POST: CPU MIC PortASIC interface Loopback Tests : Begin
POST: CPU MIC PortASIC interface Loopback Tests : End, Status Passed

POST: PortASIC RingLoopback Tests : Begin
POST: PortASIC RingLoopback Tests : End, Status Passed
```

Figura 6-4 Proceso de arranque. Salida por consola.

```
switch#show post
Stored system POST messages:

Switch 1
---------

POST: CPU MIC register Tests : Begin
POST: CPU MIC register Tests : End, Status Passed

POST: PortASIC Memory Tests : Begin
POST: PortASIC Memory Tests : End, Status Passed

POST: CPU MIC PortASIC interface Loopback Tests : Begin
POST: CPU MIC PortASIC interface Loopback Tests : End, Status Passed

POST: PortASIC RingLoopback Tests : Begin
POST: PortASIC RingLoopback Tests : End, Status Passed

POST: PortASIC CAM Subsystem Tests : Begin
POST: PortASIC CAM Subsystem Tests : End, Status Passed

POST: PortASIC Port Loopback Tests : Begin
POST: PortASIC Port Loopback Tests : End, Status Passed

switch#_
```

Figura 6-5 Proceso de arranque. Comando show post

Durante el inicio del switch, si se detectan fallos en la POST, se envía un informe a la consola, y el switch no se pone en funcionamiento. Si la prueba POST finaliza con éxito y el switch no se ha configurado previamente, será entonces cuando se le requerirá al administrador que lo haga.

La configuración de fabrica por defecto del switch o predeterminada hace que la administración del mismo sea controlada a través de la VLAN1, como demuestra la siguiente figura.

```
Would you like to terminate autoinstall? [yes]: no


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Would you like to terminate autoinstall? [yes]: no
Switch>
00:01:49: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively down
Switch>en
Switch#show vl
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

 --More--
```

Figura 6-6 Configuración de fábrica por defecto. Administración por VLAN1

6.2.2 Configuración básica de administración

Un switch de capa de acceso se parece mucho a un PC, ya que necesita que le configuren una dirección IP, una máscara de subred y un gateway predeterminado. Evidentemente para manejar un switch de forma remota mediante TCP/IP, es necesario asignar al switch una dirección IP. A continuación se detalla como llevar a cabo la configuración de estos parámetros en el switch. De este modo, el apartado se divide en los siguientes puntos:

- Conceptos básicos
- Configuración de las contraseñas para el modo EXEC
- Configuración del nombre del host
- Configuración de la IP de administración
- Configuración del gateway por defecto

6.2.2.1 Conceptos básicos

Cualquier switch Cisco permite trabajar en dos modos: usuario y privilegiado. Y además admite varios modos de configuración.

- **Modo usuario**: Permite consultar toda la información relacionada al switch sin poder modificarla. El shell es el siguiente:

```
Switch >
```

- **Usuario privilegiado**: Permite visualizar el estado del switch e importar/exportar imágenes de IOS. El shell es el siguiente:

```
Switch #
```

- **Modo de configuración global**: Permite utilizar los comandos de configuración generales del switch. El shell es el siguiente:

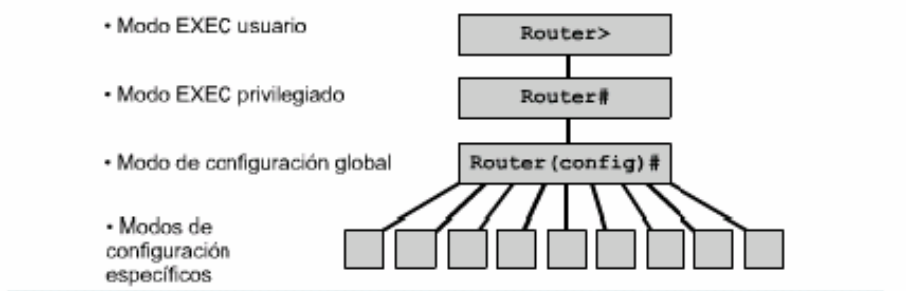
```
Switch (config) #
```

- **Modo de configuración de interfaces**: Permite utilizar comandos de configuración de interfaces (Direcciones IP, mascaras, etc.). El shell es el siguiente:

```
Switch (config-if) #
```

- **Modo de configuración de línea**: Permite configurar una línea (por ejemplo, acceso al switch por ssh). El shell es el siguiente:

```
Switch (config-line) #
```



Modo de configuración	Símbolo
Interfaz	Router(config-if)#
Subinterfaz	Router(config-subif)#
Controlador	Router(config-controller)#
Lista de mapa	Router(config-map-list)#
Clase de mapa	Router(config-map-class)#
Línea	Router(config-line)#
Router	Router(config-router)#
Router IPX	Router(config-ipx-router)#
Mapa de ruta	Router(config-route-map)#

Figura 6-7 Switch. Modos de configuración

6.2.2.2 Configuración de las contraseñas para el modo EXEC

El Modo EXEC privilegiado permite al usuario que lo habilite, configurar cualquier opción disponible en el switch y consultar todos los parámetros de la configuración en curso del switch. Por estos motivos, es importante restringir el acceso en modo EXEC privilegiado.

El comando de configuración global “enable password” permite especificar una contraseña para restringir el acceso en modo EXEC privilegiado. Sin embargo, una desventaja de este comando es que almacena la contraseña en texto legible en la configuración de inicio y en la configuración en ejecución. Como consecuencia, si alguna persona obtuviese acceso a un archivo de configuración de inicio almacenado, o bien acceso temporal a una sesión de Telnet o de consola que se encuentre en modo EXEC privilegiado, podría leer la contraseña. Para evitarlo, Cisco introdujo el comando “enable secret”, que permite controlar el acceso al modo EXEC privilegiado pero almacena de forma encriptada la contraseña especificada.

Sintaxis de comandos IOS de Cisco - Configuración de contraseñas		
1º	Cambiar de modo EXEC usuario a modo EXEC privilegiado	`Switch>enable`
2º	La petición de entrada # significa EXEC privilegiado	`Switch#`
3º	Cambiar de modo EXEC privilegiado a modo EXEC usuario	`Switch#disable`
4º	La petición de entrada > significa modo EXEC usuario	`Switch>`
5º	Contraseña enable secret	`Switch#enable secret`

Tabla 6-2 Comandos para la configuración de contraseñas

La Figura 6-8 ilustra los pasos realizados para configurar la contraseña en el switch ScSwitch12 y en la Figura 6-9 puede verse el resultado de esta acción, la contraseña enable secret encriptada.

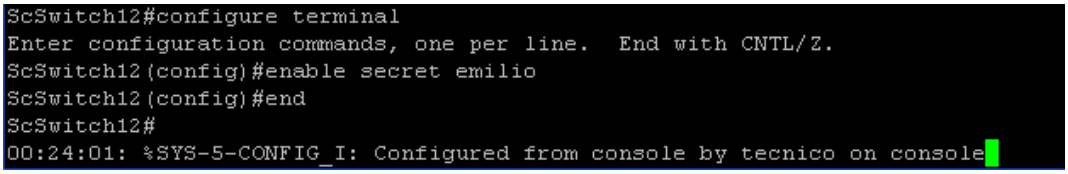


Figura 6-8 Configuración enable secret

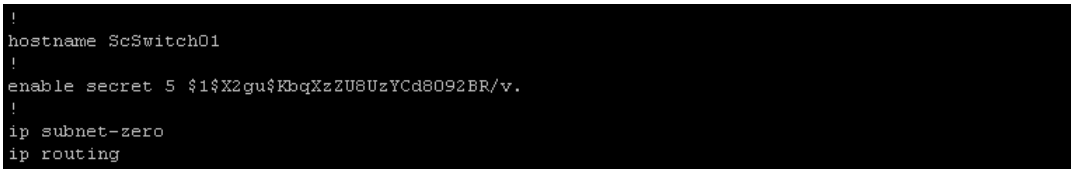


Figura 6-9 Contraseña enable secret encriptada

6.2.2.3 Configuración del Nombre del host

Sintaxis de comandos IOS de Cisco - Configurar nombre del Host		
1º	Cambiar de modo EXEC usuario a modo EXEC privilegiado	`Switch>enable`
2º	La petición de entrada # significa EXEC privilegiado	`Switch#`
3º	Modo configuración global	`Switch#configure terminal`
4º	Introducir nombre del host	`Switch(config)#hostname ScSwitch12`

Tabla 6-3 Comandos para configurar el nombre del host

6.2.2.4 Configuración de la IP de administración

Sintaxis de comandos IOS de Cisco - Configurar IP de administración		
1º	Modo configuración global	`Switch#configure terminal`
2º	Ingresar al modo de configuración de interfaz para la interfaz N	`Switch(config)#interface vlan N`
3º	Configurar la dirección IP de la interfaz	`Switch(config-if)# ip address IP MASCARA`
4º	Habilitar la interfaz	`Switch(config-if)# no shutdown`

Tabla 6-4 Comandos para configurar la IP de administración

6.2.2.5 Configuración del gateway por defecto

Sintaxis de comandos IOS de Cisco – Configurar Gateway por defecto		
1º	Modo configuración global	`Switch#configure terminal`
2º	Configurar el gateway predeterminado en el switch	`Switch(config)#ip default-gateway IP`

Tabla 6-5 Comandos para configurar el gateway por defecto.

En la Figura 6-10 se pueden observar los pasos, descritos anteriormente, que se han ejecutado para configurar los parámetros básicos del switch ScSwitch12.

```
Switch(config)#hostname ScSwitch12
ScSwitch12(config)#interface vlan 8
ScSwitch12(config-if)#ip address 10.239.71.112 255.255.255.0
ScSwitch12(config-if)#no shutdown
ScSwitch12(config-if)#exit
ScSwitch12(config)#ip default-gateway 10.239.71.1
ScSwitch12(config)#interface vlan 1
ScSwitch12(config-if)#shutdown
ScSwitch12(config-if)#exit
```

Figura 6-10 Configuración básica del switch

La Figura 6-11 muestra la salida del comando “show ip interface brief”, que permite al administrador analizar su resultado y comprobar si es el esperado para la configuración dada, lo cual sería indicativo de que el proceso se ha sido llevado a cabo con éxito.

```
ScSwitch12#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES unset  administratively down down
Vlan8                  10.239.71.112   YES manual up                    up
```

Figura 6-11 Verificación de la configuración básica del switch

6.2.3 Configuración de VLAN

6.2.3.1 Creación de VLAN en el switch

Sintaxis de comandos IOS de Cisco – Configurar VLAN		
1º	Modo configuración global	`Switch#configure terminal`
2º	Entrar en la configuración de la VLAN	`Switch(config)#ivlan N`
3º	Configurar el nombre de la VLAN	`Switch(config-vlan)#name Nombre`

Tabla 6-6 Comandos para configurar VLAN

La Figura 6-12 muestra los pasos ejecutados para crear la VLAN8 en el switch ScSwitch12.

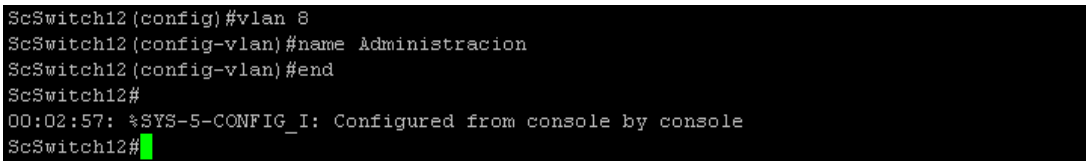


Figura 6-12 Creación de una VLAN

6.2.3.2 ¿Qué es el dominio VTP?

El VTP (VLAN Trunking Protocol) permite configurar un switch de modo que propague las configuraciones de las VLANs hacia los otros switches en la red. De este modo, el VTP permite al administrador realizar cambios en la configuración de VLANs en un switch que actúa como servidor VTP. Dicho servidor se encargará de distribuir a través de la red la información de las VLANs a los switches habilitados por el VTP, lo que minimiza errores de configuración e incoherencias en la misma, al mismo tiempo que reduce las necesidades de configuración manual de la red.

El VTP guarda las configuraciones de las VLANs en el fichero de texto vlan.dat y usa una jerarquía de publicaciones para distribuir y sincronizar la información acerca de las VLANs a través de la red. Se llama dominio VTP a uno o más switches interconectados que comparten los detalles de configuración de las VLANs a través de publicaciones VTP, es decir, que comparten el mismo entorno VTP. Un switch solo puede configurarse en un dominio VTP. El límite de cada dominio está definido por un switch de capa 3.

Las publicaciones VTP inundan el dominio cada cinco minutos o cada vez que se produzca un cambio en las configuraciones VLANs. En una publicación VTP se incluye un número de revisión de la configuración, de tal manera, que un número más alto significa que la información de las VLANs que se está publicando es más moderna que la que está almacenada.

Un switch se puede configurar para que funcione como servidor VTP, como cliente VTP, o bien como switch VTP transparente.

- **Servidor VTP.** Un switch configurado de este modo publica la información de las VLANs, pertenecientes al dominio VTP, a otros switches habilitados por el VTP en el mismo dominio. Los servidores VTP guardan la información de las VLANs para el dominio completo en la memoria de acceso aleatorio no volátil (NVRAM). Un switch operando en modo servidor VTP puede crear, modificar y borrar VLANs y otros parámetros de configuración para el dominio VTP completo. Cuando se efectúa un cambio en la configuración VLAN de un servidor VTP, éste incrementa en uno el número de revisión de la configuración y propaga el cambio a todos los switches del dominio.

- **Cliente VTP.** Un dispositivo operando en este modo no puede crear, cambiar, ni eliminar VLANs. Un cliente VTP sólo guarda la información de la VLAN para el dominio completo mientras el switch está activado, pero no la almacena en la memoria no volátil, por tanto, un reinicio del switch borra la información de VLANs. Es necesario establecer como cliente VTP cualquier switch en el que el administrador no quiera crear, cambiar o borrar VLANs.

- **VTP transparente**. Los switches en modo VTP transparente no crea publicaciones VTP ni sincroniza su configuración VLAN con la información recibida de otros switches del dominio, solo envía las publicaciones VTP recibidas de otros switches que forman parte del mismo dominio a los clientes y servidores VTP. Puede crear, eliminar y modificar VLANs, pero los cambios no se transmiten a los otros switches del dominio, solo afectan al switch local.

La siguiente tabla ofrece una comparativa de los tres modos VTP.

Modos VTP		
Modo servidor	**Modo cliente**	**Modo transparente**
Envía/reenvía publicaciones VTP	Envía/reenvía publicaciones VTP	Reenvía publicaciones VTP
Sincroniza la información de la configuración VTP con los otros switches	Sincroniza la información de la configuración VTP con los otros switches	No sincroniza la información de la configuración VTP con los otros switches
El switch catalyst puede crear VLAN	El switch catalyst no puede crear VLAN	El switch catalyst puede crear VLAN
El switch catalyst puede modificar VLAN	El switch catalyst no puede modificar VLAN	El switch catalyst puede modificar VLAN
El switch catalyst puede eliminar VLAN	El switch catalyst no puede eliminar VLAN	El switch catalyst puede eliminar VLAN

Tabla 6-7 Modos VTP

6.2.3.3 Comandos para la configuración de VTPs

Sintaxis de comandos IOS de Cisco – Configurar VTP		
1º	Modo configuración global	`Switch#configure terminal`
2º	Ingresar el modo de operación, servidor, cliente o transparente la interfaz para asignar la VLAN	`Switch(config)#vtp mode [server|client|transparent] DOMINIO`

3º	Definir la versión	`Switch(config-if)# vtp version [1|2]`
4º	Configurar la contraseña de VTP	`Switch(config-if)# vtp password contraseña`

Tabla 6-8 Comandos para configurar VTP

En el IATE los switches ScSwich01 y ScSwitch02 se han configurado como servidores VTP, los switches de la VLAN de servidores en modo VTP transparente, y el resto como cliente VTP. La siguiente figura refleja este escenario.

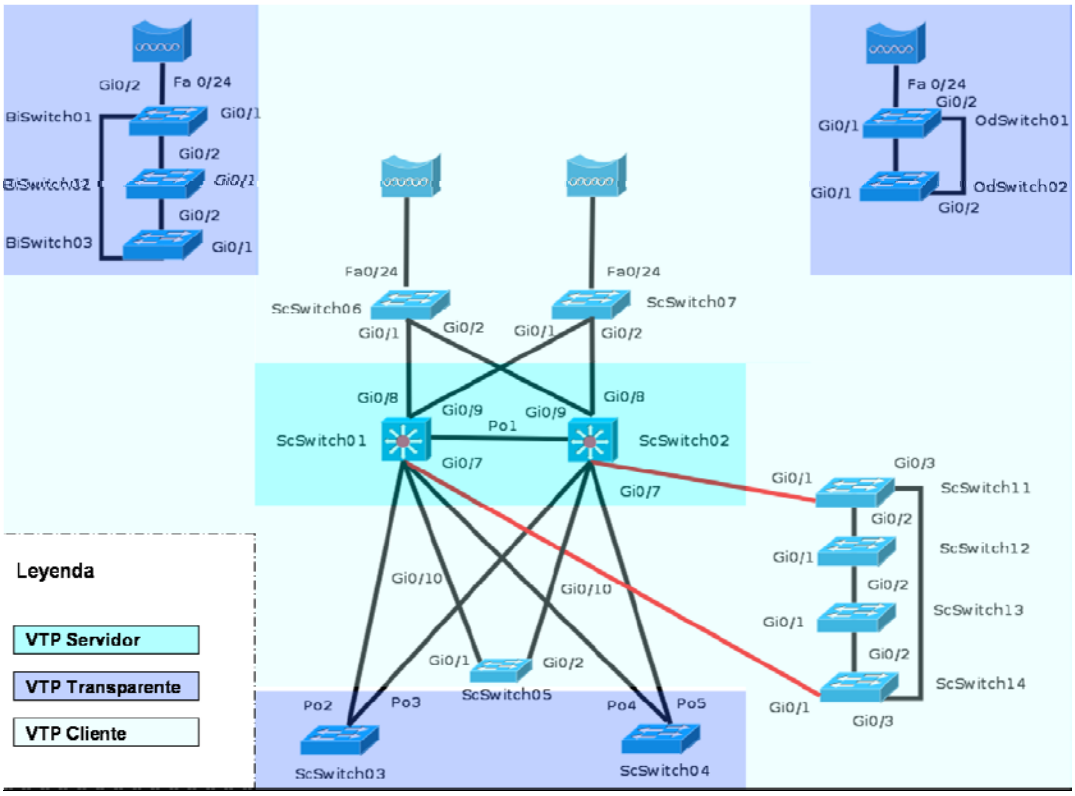


Figura 6-13 Reparto de modos VTP en el IATE

Siguiendo con el switch ScSwitch12, a continuación se muestran los comandos ejecutados para configurarlo como cliente VTP.

```
ScSwitch12(config)#vtp mode client
Device mode already VTP CLIENT.
ScSwitch12(config)#vtp version 2
Cannot modify version in VTP client mode
ScSwitch12(config)#vtp domain IATE
Domain name already set to IATE.
ScSwitch12(config)#vtp password mcmlredr
Setting device VLAN database password to mcmlredr
ScSwitch12(config)#
```

Figura 6-14 Configurar Cliente VTP

El comando “show vlan” permite comprobar que el cliente VTP ha recibido una publicación VTP, demostrando que conoce la información de las VLANs, como se observa en la figura.

```
ScSwitch12#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Gi0/1
                                                Gi0/2
2    Informatica                      active
3    Olive                            active
4    Servidores                       active
5    Bilbao                           active
6    Odonell                          active
7    Wireless                         active
8    Administracion                   active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

Figura 6-15 Publicación VTP recibida por el cliente

6.2.4 Configuración de Puertos

En primer lugar, el administrador pone todos los puertos a shudown, para evitar que nadie se conecte sin autorización.

```
ScSwitch12(config)#interface range fastEthernet 0/1 - 24
ScSwitch12(config-if-range)#shutdown
ScSwitch12(config-if-range)#exit
ScSwitch12(config)#end
ScSwitch12#
ScSwitch12#
00:58:07: %SYS-5-CONFIG_I: Configured from console by console
```

Figura 6-16 Puertos a shutdown

La Figura 6-17 muestra la salida del comando “show interfaces status”, que permite al administrador ver el estado de las interfaces. En este caso están todas deshabilitadas, lo cual es indicativo de que el proceso de shutdown ha sido llevado a cabo con éxito.

```
ScSwitch12#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        disabled     1            auto   auto 10/100BaseTX
Fa0/2                        disabled     1            auto   auto 10/100BaseTX
Fa0/3                        disabled     1            auto   auto 10/100BaseTX
Fa0/4                        disabled     1            auto   auto 10/100BaseTX
Fa0/5                        disabled     1            auto   auto 10/100BaseTX
Fa0/6                        disabled     1            auto   auto 10/100BaseTX
Fa0/7                        disabled     1            auto   auto 10/100BaseTX
Fa0/8                        disabled     1            auto   auto 10/100BaseTX
Fa0/9                        disabled     1            auto   auto 10/100BaseTX
Fa0/10                       disabled     1            auto   auto 10/100BaseTX
Fa0/11                       disabled     1            auto   auto 10/100BaseTX
Fa0/12                       disabled     1            auto   auto 10/100BaseTX
Fa0/13                       disabled     1            auto   auto 10/100BaseTX
Fa0/14                       disabled     1            auto   auto 10/100BaseTX
```

Figura 6-17 Puertos deshabilitados

La siguientes tablas resumen los comandos necesarios para configurar los puertos de acceso y troncales, respectivamente.

Sintaxis de comandos IOS de Cisco – Configurar los puertos de acceso		
1º	Modo configuración global	`Switch#configure terminal`
2º	Ingresar en la interfaz para asignar la VLAN	`Switch(config)#interface fastethernet 0/N`
3º	Definir el modo de membresia de la VLAN para el puerto	`Switch(config-if)# switchport mode access`
4º	Asignar el puerto a una VLAN	`Switch(config-if)# switchport access vlan X`

Tabla 6-9 Comandos para configurar los puertos de acceso

Sintaxis de comandos IOS de Cisco – Configurar los puertos troncales		
1º	Modo configuración global	`Switch#configure terminal`
2º	Ingresar en la interfaz para asignar la VLAN	`Switch(config)#interface fastethernet 0/N`
3º	Definir el modo trunk	`Switch(config-if)# switchport mode trunk`

Tabla 6-10 Comandos para configurar los puertos troncales

Como se dijo al comienzo del capitulo, la configuración de fábrica por defecto del switch o predeterminada hace que la administración del mismo sea controlada a través de la VLAN1. Sin embargo, una optimización a la configuración predeterminada del switch consiste en modificar la administración para que la realice una VLAN que no sea la VLAN1. Las implicaciones y razones de esta acción se explicaron en el capitulo de seguridad.

En la Figura 6-18 se puede ver como se sitúan los puertos del switch ScSwitch12 en la VLAN de Muñoz Olivé, VLAN3, que es donde está ubicado. Seguidamente se crea el puerto troncal en la interfaz Gi0/1

```
ScSwitch12#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch12(config)#interface range fastEthernet 0/1 - 24
ScSwitch12(config-if-range)#switchport mode access
ScSwitch12(config-if-range)#switchport access vlan 3
ScSwitch12(config-if-range)#exit
ScSwitch12(config)#
ScSwitch12(config)#
ScSwitch12(config)#interface gigabitEthernet 0/1
ScSwitch12(config-if)#switchport mode trunk
ScSwitch12(config-if)#spanning-tree link-type point-to-point
ScSwitch12(config-if)#end
ScSwitch12#
```

Figura 6-18 Asignación de puertos a VLAN 3 y creación de puertos troncales

La Figura 6-19 muestra la salida del comando "show interfaces status", que permite al administrador comprobar que efectivamente los puertos están asignados a la VLAN3.

```
ScSwitch12#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        disabled     3            auto   auto 10/100BaseTX
Fa0/2                        disabled     3            auto   auto 10/100BaseTX
Fa0/3                        disabled     3            auto   auto 10/100BaseTX
Fa0/4                        disabled     3            auto   auto 10/100BaseTX
Fa0/5                        disabled     3            auto   auto 10/100BaseTX
Fa0/6                        disabled     3            auto   auto 10/100BaseTX
Fa0/7                        disabled     3            auto   auto 10/100BaseTX
Fa0/8                        disabled     3            auto   auto 10/100BaseTX
Fa0/9                        disabled     3            auto   auto 10/100BaseTX
Fa0/10                       disabled     3            auto   auto 10/100BaseTX
Fa0/11                       disabled     3            auto   auto 10/100BaseTX
Fa0/12                       disabled     3            auto   auto 10/100BaseTX
Fa0/13                       disabled     3            auto   auto 10/100BaseTX
Fa0/14                       disabled     3            auto   auto 10/100BaseTX
Fa0/15                       disabled     3            auto   auto 10/100BaseTX
Fa0/16                       disabled     3            auto   auto 10/100BaseTX
Fa0/17                       disabled     3            auto   auto 10/100BaseTX
Fa0/18                       disabled     3            auto   auto 10/100BaseTX
Fa0/19                       disabled     3            auto   auto 10/100BaseTX
Fa0/20                       disabled     3            auto   auto 10/100BaseTX
Fa0/21                       disabled     3            auto   auto 10/100BaseTX
```

Figura 6-19 Verificación de la asignación de puertos a VLAN3

6.2.5 Configuración de Seguridad

En este apartado se van a tratar los siguientes puntos:

- Configuración del acceso a la consola
- Protección de los puertos VTY (Virtual Terminal)
- Configuración ssh
- Mensajes de inicio de sesión
- Seguridad en puerto
- ACL (Access Control List)

6.2.5.1 Configuración del acceso a la consola

Sintaxis de comandos IOS de Cisco – Configurar el acceso a la línea de consola		
1º	Modo configuración global	`Switch#configure terminal`
2º	Ingresar en la línea de consola	`Switch(config)#line console 0`
3º	Definir el modo trunk	`Switch(config-line)# login local`

Tabla 6-11 Comandos la línea de consola

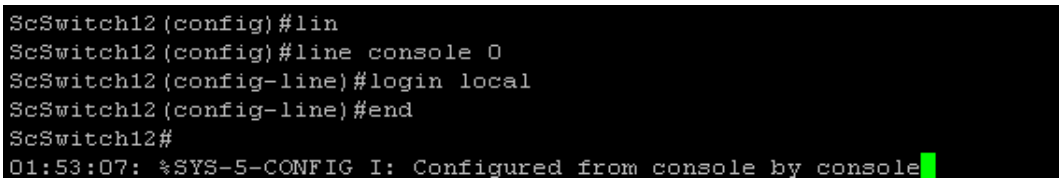


Figura 6-20 Configuración del puerto de consola

6.2.5.2 Protección de los puertos VTY

Los puertos VTY de un switch Cisco permiten obtener acceso remoto al dispositivo. Es posible llevar a cabo todas las opciones de configuración mediante los puertos de terminal VTY, y no es necesario acceder físicamente al switch para obtener acceso a dichos puertos. Por ello, es muy importante que estén protegidos. Cualquier usuario con acceso de red al switch puede establecer una conexión remota de terminal VTY. Si no se aseguran los puertos VTY de forma adecuada, usuarios malintencionados podrían comprometer la configuración del switch.

Un switch de Cisco puede contar con varios puertos vty disponibles, de manera que más de un administrador pueda conectarse y administrar el switch. Para proteger todas las líneas VTY, hay que asegurarse de que se establezca una contraseña y que el inicio de sesión sea obligatorio en todas las líneas. La falta de protección en algunas líneas compromete la seguridad y permite el acceso no autorizado al switch.

Sintaxis de comandos IOS de Cisco – Configurar las líneas de terminal		
1º	Modo configuración global	`Switch#configure terminal`
2º	Ingresar en la línea de consola	`Switch(config)#line vty 0 15`
3º	Definir el trafico que se va a permitir	`Switch(config-line)#trnasport {input | output | preferred} {all | none | ssh | Telnet}`
4º	Definir el modo trunk	`Switch(config-line)# login local`

Tabla 6-12 Configuración de VTY

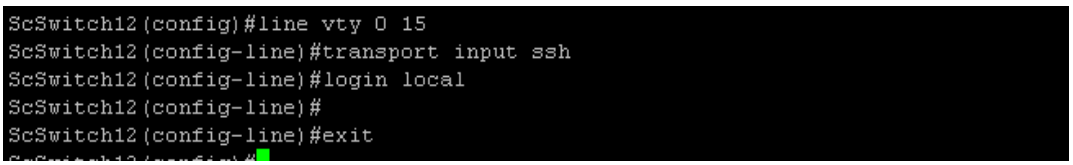


Figura 6-21 Configuración de las líneas VTY

6.2.5.3 Configuración ssh

Sintaxis de comandos IOS de Cisco – Configurar SSH		
1º	Modo configuración global	`Switch#configure terminal`
2º	Definir el nombre del router	`Switch(config)#hostname NombreHost`
3º	Configurar el nombre de dominio	`Switch(config-if)# ip domain-name NombreDominio`
4º	Habilitar el servidor SSH para la autenticación remota y local en el switch, y generar un par de claves RSA	`Switch(config-if)# crypto key generate rsa`
5º	Habilitar versión 2	`Switch(config)#ip ssh version 2`
6º	Definir los tiempos de inactividad	`Switch(config-if)#ip ssh time-out N`
7º	Definir el numero de intentos de acceso al switch	`Switch(config-if)#ip ssh authentication-retries N`
8º	Definición de usuarios	`Switch(config)#Username nombre secret contraseña`

9º	Configuración terminales	`Switch(config)#line vty 0 15`
		`Switch(config-line)#transport input ssh`
		`Switch(config-line)#login local`

Tabla 6-13 Comandos para configurar SSH

```
ScSwitch12#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch12(config)#hostname ScSwitch12
ScSwitch12(config)#ip domain-name iate.junta-andalucia.es
ScSwitch12(config)#crypto key generate rsa
The name for the keys will be: ScSwitch12.iate.junta-andalucia.es
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys ...[OK]

ScSwitch12(config)#
01:43:54: %SSH-5-ENABLED: SSH 1.99 has been enabled
ScSwitch12(config)#ip ssh version 2
ScSwitch12(config)#ip ssh time-out 90
ScSwitch12(config)#ip ssh authentication-retries 3
ScSwitch12(config)#username tecnico secret emilio
```

Figura 6-22 Configuración de SSH

6.2.5.4 Mensajes de inicio de sesión y mensajes del día

El conjunto de comandos IOS de Cisco incluye una característica que permite configurar los mensajes que cualquier persona puede ver cuando inicia sesión en el switch. Estos mensajes pueden ser del tipo mensajes de inicio de sesión o bien mensajes del día (MOTD).

El usuario puede definir un mensaje personalizado para que se muestre antes de la petición de contraseña, utilizando el comando “banner login” en el modo de configuración global y el texto del mensaje entre comillas o bien un delimitador diferente a cualquier carácter que aparece en la cadena del mensaje MOTD.

El mensaje MOTD se muestra en todos los terminales conectados durante el inicio de sesión y es útil para enviar mensajes que afectan a todos los usuarios de la red (como desconexiones inminentes del sistema). Si se configura, el mensaje MOTD se muestra antes del mensaje de inicio de sesión.

Sintaxis de comandos IOS de Cisco – Configurar mensajes de inicio de sesión		
1º	Modo configuración global	`Switch#configure terminal`
2º	Configurar un mensaje de inicio de sesión	`Switch(config)#banner login “TEXTO”`

Tabla 6-14 Comandos para configurar mensajes de inicio de sesión

Sintaxis de comandos IOS de Cisco – Configurar mensajes MOTD		
1º	Modo configuración global	`Switch#configure terminal`
2º	Configurar un mensaje del día	`Switch(config)#banner motd “TEXTO”`

Tabla 6-15 Comandos para configurar mensajes MOTD

En la siguiente figura se muestra como configurar el switch ScSwitch12 para que muestre el mensaje “Queda prohibido el acceso no autorizado” al inicio de sesión.

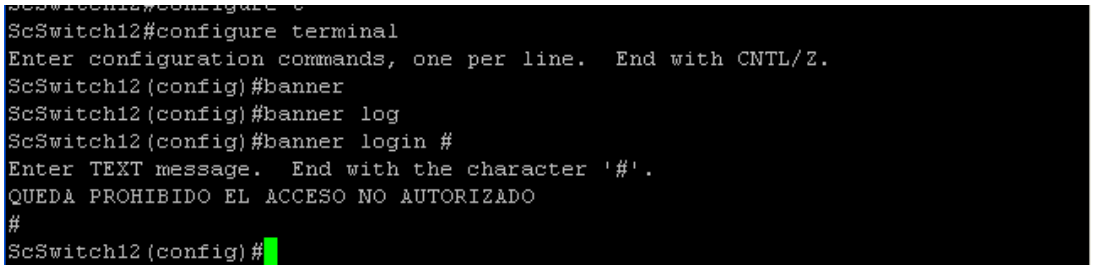


Figura 6-23 Configuración de un mensaje de inicio de sesión

6.2.5.5 Seguridad en puerto

Sintaxis de comandos IOS de Cisco – Configurar seguridad en puerto		
1º	Modo configuración global	`Switch#configure terminal`
2º	Especificar el tipo y numero de interfaz física a configurar	`Switch(config)#interface fastEthernet 0/N`

3º	Establecer el modo de interfaz como acceso.	`Switch(config-if)#switchport mode access`
4º	Activar la seguridad de puerto en la interfaz	`Switch(config-if)#switchport port-security`
5º	Establecer el numero máximo de direcciones seguras	`Switch(config-if)#switchport port-security maximum N`
6º	Activar el aprendizaje sin modificaciones.	`Switch(config-if)#switchport port-security mac-address sticky`
7º	Si se produce una violación de puerto, éste se pone a shutdown	`Switch(config-if)#switchport port-security violation shutdown`

Tabla 6-16 Comandos para configurar la seguridad en puerto

```
ScSwitch12#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch12(config)#interface fastethernet 0/1
ScSwitch12(config-if)#switchport port-security maximum 1
ScSwitch12(config-if)#switchport port-security mac-address sticky
ScSwitch12(config-if)#switchport port-security violation shutdown
ScSwitch12(config-if)#end
ScSwitch12#
```

Figura 6-24 Configuración de port-security

6.2.5.6 Configuración del DHCP Snooping

Sintaxis de comandos IOS de Cisco – Configurar DHCP Snooping		
1º	Modo configuración global	`Switch#configure terminal`
2º	Habilitar DHCP Snooping	`Switch(config)#ip dhcp snooping`
3º	Habilitar la opción 82 del DHCP	`Switch(config)#ip dhcp snooping information option`
4º	Configurar las interfaces que son de confianza	`Switch(config)#ip dhcp snooping trust`
5º	Configurar el numero de paquetes por segundo aceptado por el Puerto	`Switch(config)#ip dhcp snooping limit rate [numero]`
6º	Habilitar DHCP snooping por VLAN	`Switch(config)#ip dhcp snooping vlan number [id-vlan]`

Tabla 6-17 Comandos para configurar DHCP Snooping

Continuando con la configuración del switch ScSwitch12, la Figura 6-25 ilustra los comandos ejecutados para configurar el DHCP Snooping en un switch de capa 2. Más adelante se llevará a cabo la misma tarea para configurar esta característica en el switch de capa 3.

```
ScSwitch12#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch12(config)#ip dhcp snooping
ScSwitch12(config)#ip dhcp snooping information option
ScSwitch12(config)#interface range gigabitEthernet 0/1 - 2
ScSwitch12(config-if-range)#ip dhcp snooping trust
ScSwitch12(config-if-range)#exit
ScSwitch12(config)#interface range fastEthernet 0/1 -24
ScSwitch12(config-if-range)#ip dhcp snooping limit rate 15
ScSwitch12(config-if-range)#exit
ScSwitch12(config)#ip dhcp snooping vlan 3
ScSwitch12(config)#end
```

Figura 6-25 Configuración de DHCP Snooping en un switch de capa 2

6.2.5.7 Configuración de ACL

Sintaxis de comandos IOS de Cisco – Lista de acceso Estándar		
1º	Modo configuración global	`Switch#configure terminal`
2º	Crear la lista de acceso estándar	`Switch(config)#access-list N {permit|deny} direccion_origen [mascara-wildcard]`
3º	Aplicación de la ACL	`Switch(config)#interface interfaz-aplicar` `Switch(config-if)#ip access-group N {in | out }`

Tabla 6-18 Comandos para configurar ACL Estándar

Sintaxis de comandos IOS de Cisco – Lista de acceso Extendida		
1º	Modo configuración global	`Switch#configure terminal`
2º	Crear la lista de acceso extendida	`Switch(config)#access-list N {permit|deny} protocolo dirección-origen wildcard-origen [operador Puerto] direccion-destino wildcard-destino [operador Puerto]`
3º	Aplicación de la ACL	`Switch(config)#interface interfaz-aplicar` `Switch(config-if)#ip access-group N {in | out }`

Tabla 6-19 Comandos para configurar ACL Extendida

Sintaxis de comandos IOS de Cisco – Lista de acceso con nombre		
1º	Modo configuración global	`Switch#configure terminal`
2º	Crear la lista de de acceso extendida	`Switch(config)#access-list {standard | extended} nombre_acl` `Switch(config)#{access-list standard`

		`| acces-list extended} { permit – deny} { condiciones pruebas }`
3º	Aplicación de la ACL	`Switch(config)#interface interfaz-aplicar` `Switch(config-if)#ip access-group nombre_acl {in | out }`

Tabla 6-20 Comandos para configurar ACL con nombre

Sintaxis de comandos IOS de Cisco – Lista de acceso para la VTY		
1º	Modo configuración global	`Switch#configure terminal`
2º	Crear la lista de de acceso extendida	`Switch(config)#access-list {standard | extended} nombre_acl` `Switch(config)#{access-list standard | acces-list extended}`
3º	Aplicación de la ACL	`Switch(config)#line vyt 0 15` `Switch(config-if)#ip access-class acl {in | out }`

Tabla 6-21 Comandos para configurar ACL para la VTY

```
ScSwitch12(config)#access-list 1 permit 10.239.65.0 0.0.0.255
ScSwitch12(config)#
ScSwitch12(config)#line vty 0 15
ScSwitch12(config-line)# access-class 1 in
ScSwitch12(config-line)#end
ScSwitch12#
```

Figura 6-26 Configuración del acceso a la línea VTY

Las ACL protegen el acceso a las líneas VTY y controlan el tráfico entrante y saliente. La Figura 6-27 ilustra como configurar una ACL que garantice el cumplimiento del requisito REQ_14, visto en el capítulo 4, según el cual el administrador debe asegurar que el acceso a la línea de la terminal solo se puede realizar desde la VLAN de informática.

```
ScSwitch12#
ScSwitch12#show access-list 1
Standard IP access list 1
    10 permit 10.239.65.0, wildcard bits 0.0.0.255
ScSwitch12#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch12(config)#line vty 0 15
ScSwitch12(config-line)#access-class 1 in
ScSwitch12(config-line)#end
ScSwitch12#
```

Figura 6-27 Restringir el acceso a la VLAN de informática

6.2.6 Configuración de STP

6.2.6.1 Configuración de Rapid-PVST

Sintaxis de comandos IOS de Cisco – Configurar Rapid-PVST		
1º	Modo configuración global	`Switch#configure terminal`
2º	Configurar el modo Rapid PVST más Spanning Tree	`Spanning-tree mode rapid-pvst`
3º	Ingresar en el modo de configuración de interfaz y especificar una interfaz para configurar.	`Interface interface-id`
4º	Especificar que el tipo de enlace para este puerto es punto a punto	`Spanning-tree link-type point-to-point`
5º	Borrar todos los STP detectados	`Clear spanning-tree detected-protocols`

Tabla 6-22 Comandos para configurar Rapid-PVST

```
ScSwitch12#
ScSwitch12#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch12(config)#spanning-tree mode rapid-pvst
ScSwitch12(config)#interface range gigabitEthernet 0/1 - 2
ScSwitch12(config-if-range)#switchport mode trunk
ScSwitch12(config-if-range)#spanning-tree link-type point-to-point
ScSwitch12(config-if-range)#end
ScSwitch12#
ScSwitch12#
```

Figura 6-28 Configuración de Rapid-PVST

6.2.6.2 Configuración de Portfast/BPDU Guard

Sintaxis de comandos IOS de Cisco – Configurar Portfast/BPDU Guard		
1º	Modo configuración global	`Switch#configure terminal`
2º	Configurar el modo Rapid PVST más Spanning Tree	`Spanning-tree mode rapid-pvst`
3º	Ingresar en el modo de configuración de interfaz y especificar una interfaz para configurar.	`Switch(config)#Interface interface-id`
4º	Especificar la configuración del puerto de extremo	`Switch(config-if)#spanning-tree portfast`
5º	Activar la protección BPDU Guard	`Switch(config-if)#spanning-tree portfast bpduguard enable`

Tabla 6-23 Comandos para configurar Portfast/BPDU Guard

```
ScSwitch12(config)#interface fastEthernet 0/1
ScSwitch12(config-if)#spanning-tree portfast
ScSwitch12(config-if)#spanning-tree bpduguard enable
ScSwitch12(config-if)#end
ScSwitch12#
```

Figura 6-29 Configuración de Portfast/BPDU Guard

6.2.7 Monitorización

6.2.7.1 NTP

Una especificación de tiempo precisa es importante para conseguir una correcta auditoría y administración. NTP proporciona una base de tiempo común para los switches, servidores y otros dispositivos de la red.

Un sistema de tiempo sincronizado habilita la correlación del Syslog y las salidas de Debug del Cisco IOS para eventos específicos.

Sintaxis de comandos IOS de Cisco – Configurar NTP		
1º	Modo configuración global	`Switch#configure terminal`
2º	Configurar el switch como cliente NTP	`Switch(config)# ntp Server { ip-address | hostname}`

Tabla 6-24 Comandos para configurar NTP

6.2.7.2 Loggin

Los switches Cisco pueden enviar sus mensajes de log a un servicio Syslog al estilo UNIX. Este servicio simplemente acepta los mensajes y los almacena en archivos o los imprime en función de lo especificado en un fichero de configuración, como se verá en el siguiente capítulo.

Cualquier administrador de seguridad de red debe siempre registrar los eventos significativos en un servidor de Syslog, el cual debe estar localizado en una red interna segura para garantizar la integridad del log. Por tanto, es necesaria tanto la configuración de la electrónica de red Cisco, que actuará como cliente, como la del servidor Syslog.

En este punto se describe como configurar un switch cliente, mientras que la configuración del servidor de Syslog se tratará en el siguiente capítulo.

Sintaxis de comandos IOS de Cisco – Configurar Loggin		
1º	Modo configuración global	`Switch#configure terminal`
2º	Establecer el host de destino	`Switch(config)#logging [host-name | ip-address]`
3º	Establecer el nivel de criticidad	`Switch(config)#logging trap nivel`
4º	Activar el logado	`Switch(config)#logging on`

Tabla 6-25 Comandos para configurar loggin

La siguiente figura ilustra los pasos seguidos para configurar NTP y loggin en el switch ScSwitch12, del modo descrito en las tablas anteriores.

```
ScSwitch12#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch12(config)#ntp server 10.239.71.103
ScSwitch12(config)#end
ScSwitch12#
01:54:23: %SYS-5-CONFIG_I: Configured from console by tecnico on console
ScSwitch12#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch12(config)#loggin host 10.239.67.108
ScSwitch12(config)#loggin trap informational
ScSwitch12(config)#loggin on
ScSwitch12(config)#
```

Figura 6-30 Configuración de NTP y loggin

Es posible crear un retraso entre intentos de loggin repetidos e incluso mensajes Syslog cuando un intento de loggin satisfactorio o fallido ocurre. Sin embargo, estas medidas de seguridad no están habilitadas por defecto.

Sintaxis de comandos IOS de Cisco – Habilitar medidas de seguridad para líneas VTY		
1º	Especificar el número de intentos de loggin fallidos dentro de un periodo de tiempo específico, durante el cual los intentos de loggin serán bloqueados.	`Switch(config)#login block-for <segundos> attempts <intentos> within <segundos>`
2º	Crear un log cuando intentos de loggin han sido satisfactorios o fallidos.	`Switch# Sw(config)#login on-<success | failure> log`

Tabla 6-26 Comandos para habilitar medidas de seguridad en líneas VTY

En la Figura 6-31 se define que el acceso se bloquee durante 180 segundos cuando se produzcan 3 intentos fallidos en un intervalo de 10 segundos. Además se crea un registro de Syslog con los intentos que se han sido satisfactorios y fallidos.

```
ScSwitch12(config)#login block-for 180 attempts 3 within 10
ScSwitch12(config)#login on-failure log
ScSwitch12(config)#login on-success log
ScSwitch12(config)#end
ScSwitch12#
```

Figura 6-31 Habilitar medidas de seguridad en líneas VTY

6.3 Configuración del Switch de capa 3

Además de todo lo visto hasta el momento, en los switches de capa 3 existen otras opciones a configurar, entre las que se encuentran:

- Habilitar las funciones de capa 3
- Configuración de VLAN
- Creación del dominio VTP
- Configuración del puente raíz
- Configuración de puertos enrutados
- Configuración de la ruta por defecto
- Configuración HSRP
- Configuración SVI
- Configuración RACLS y VACL
- Configuración DHCP
    - Reserva de IP por MAC
    - Excluir rangos de IP en el DHCP
    - Configuración DHCP Snooping
- Configuración de las interfaces
    - Etherchannel
    - Puertos spam

Para elaboración de este apartado se haya elegido el switch de capa 3, ScSwitch01, que se encuentra en el CPD de SS.CC. Evidentemente, durante el desarrollo del presente proyecto fin de carrera, el proceso aquí descrito se ha repetido para el switch ScSwitch02.

6.3.1 Habilitar las funciones de capa 3

Sintaxis de comandos IOS de Cisco – Habilitar funciones de capa 3		
1º	Modo configuración global	`Switch#configure terminal`
2º	Habilitar el enrutamiento de capa 3	`Switch(config)#ip routing`

Tabla 6-27 Comandos para habilitar las funciones de capa 3

6.3.2 Configuración de VLAN

Tanto para los switches de capa 2 como para los de capa 3, los comandos para configurar VLANs son los mismos, y se trataron en la Tabla 6-6 del presente capitulo. En aquel momento se describieron los pasos para la configuración de un switch de capa 2, ScSwitch12, y en esta ocasión la siguiente figura muestra el proceso para un switch de capa 3, ScSwitch01.

En la misma figura se puede apreciar que se han habilitado las funciones de enrutamiento a través del comando “ip routing”.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hos
Switch(config)#hostname ScSwitch01
ScSwitch01(config)#ip routing
ScSwitch01(config)#interface vlan 2
ScSwitch01(config-if)#ip address 10.239.65.2 255.255.255.0
ScSwitch01(config-if)#no shutdown
ScSwitch01(config-if)#exit
ScSwitch01(config)#interface vlan 3
ScSwitch01(config-if)#ip address 10.239.66.2 255.255.255.0
ScSwitch01(config-if)#no shutdown
ScSwitch01(config-if)#exit
ScSwitch01(config)#interface vlan 4
ScSwitch01(config-if)#ip address 10.239.67.2 255.255.255.0
ScSwitch01(config-if)#no shutdown
ScSwitch01(config-if)#exit
ScSwitch01(config)#interface vlan 5
ScSwitch01(config-if)#ip address 10.239.68.2 255.255.255.0
ScSwitch01(config-if)#no shutdown
ScSwitch01(config-if)#exit
ScSwitch01(config)#interface vlan 6
ScSwitch01(config-if)#ip address 10.239.69.2 255.255.255.0
ScSwitch01(config-if)#no shutdown
ScSwitch01(config-if)#exit
ScSwitch01(config)#interface vlan 7
ScSwitch01(config-if)#ip address 10.239.70.2 255.255.255.0
ScSwitch01(config-if)#shutdown
ScSwitch01(config-if)#exit
ScSwitch01(config)#interface vlan 8
ScSwitch01(config-if)#ip address 10.239.71.2 255.255.255.0
ScSwitch01(config-if)#no shutdown
ScSwitch01(config-if)#exit
ScSwitch01(config)#interface vlan 1
ScSwitch01(config-if)#shutdown
ScSwitch01(config-if)#end
ScSwitch01#
```

Figura 6-32 Creación de las VLAN

6.3.3 Creación del dominio VTP

Durante el proceso de configuración del switch ScSwitch12 se detallaron los pasos para configurar un cliente VTP. Ahora en este punto se describe como llevar a cabo la misma tarea para un servidor VTP, ya que tanto el switch ScSwitch01 como el de backup, operan en modo servidor VTP. Los comandos a emplear son los mismos que para la configuración del cliente y se ofrecieron en la Tabla 6-8 de este capitulo.

```
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch01(config)#vtp mode server
Device mode already VTP SERVER.
ScSwitch01(config)#vtp version 2
VTP mode already in V2.
ScSwitch01(config)#vtp domain IATE
Domain name already set to IATE.
ScSwitch01(config)#vtp password mcmlredr
Password already set to mcmlredr
ScSwitch01(config)#end
```

Figura 6-33 Creación del dominio VTP

6.3.4 Configuración del puente raíz

El switch ScSwitch01 es el puente raíz de la topología de Spanning Ttree, y el switch mientras que el ScSwitch02 tiene el rol de backup, en caso de que el raíz caiga éste tomará el rol de puente raíz.

Sintaxis de comandos IOS de Cisco – Configurar puente raíz		
1º	Modo configuración global	`Switch#configure terminal`
2º	Configurar el modo Rapid PVST más Spanning Tree	`Switch(config)#Spanning-tree mode rapid-pvst`
3º	Opción 1: Configurar el puente raíz	`Opción 1:` `Switch(config)#spanning-tree vlan N root { primary | secondary }`
	Opción 2: Configurar el puente raíz con prioridad 0	`Opción 2:` `Switch(config)#spanning-tree vlan N priority 0-61440`

Tabla 6-28 Comandos para configurar el puente raíz

```
ScSwitch01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch01(config)#spanning-tree mode rapid-pvst
ScSwitch01(config)#spanning-tree vlan 1-8 root primary
ScSwitch01(config)#end
ScSwitch01#
```

Figura 6-34 Configuración del puente raíz

```
ScSwitch01(config)#spanning-tree mode rapid-pvst
ScSwitch01(config)#spanning-tree vlan 2-8 priority 0
ScSwitch01(config)#end
ScSwitch01#
000024: *Mar  1 00:05:05: %SYS-5-CONFIG_I: Configured from console by c
```

Figura 6-35 Configuración del puente raíz con prioridad cero

6.3.5 Configuración de puertos enrutados

Sintaxis de comandos IOS de Cisco – Configurar puertos enrutados		
1º	Modo configuración global	`Switch#configure terminal`
2º	Deshabilitar el modo switchport en la interfaz	`Switch(config-if)#no switchport`
3º	Asignar una dirección IP a la interfaz	`Switch(config-if)#ip address ip-address mask`

Tabla 6-29 Comandos para configurar puertos enrutados

```
ScSwitch01(config)#interface gigabitEthernet 0/23
ScSwitch01(config-if)#no switchport
ScSwitch01(config-if)#ip address 10.239.128.2 255.255.255.0
ScSwitch01(config-if)#end
ScSwitch01#
```

Figura 6-36 Configuración puertos enrutados

6.3.6 Configuración de la ruta por defecto

Sintaxis de comandos IOS de Cisco – Configurar ruta por defecto		
1º	Modo configuración global	`Switch#configure terminal`
2º	Ruta por defecto	`Switch(config)#ip route 0.0.0.0 0.0.0.0 IP`

Tabla 6-30 Comandos para configurar ruta por defecto

```
ScSwitch01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch01(config)#ip route 0.0.0.0 0.0.0.0 10.239.128.4
ScSwitch01(config)#
```

Figura 6-37 Configuración ruta por defecto

6.3.7 Configuración HSRP

Sintaxis de comandos IOS de Cisco – Configurar HSRP		
1º	Modo configuración global	`Switch#configure terminal`
2º	Habilitar HSRP en la interfaz	`Switch(config-if)#standby group-number ip ip-address`
3º	Establecer una prioridad al grupo HSRP	`Switch(config-if)#standby group-number priority priority-value`
4º	Configurar HSRP para que el router activo tome el control si ha pasado a standby	`Switch(config-if)#standby [group-number] track interface prioridad`
5º	Configuración de preemt	`Switch(config-if)#standby [group-number] preempt`
6º	Configuración de la interfaz de track	`Switch(config-if)#standy [Group-number] track interface prioridad`

Tabla 6-31 Comandos para configurar HSRP

```
ScSwitch01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch01(config)#interface vlan 2
ScSwitch01(config-if)# ip address 10.239.65.2 255.255.255.0
ScSwitch01(config-if)# standby 2 ip  10.239.65.1
ScSwitch01(config-if)# standby 2 priority 200
ScSwitch01(config-if)# standby 2 preempt
ScSwitch01(config-if)# standby 2 track fastEthernet 0/23 150
ScSwitch01(config-if)#interface vlan 3
ScSwitch01(config-if)# ip address 10.239.66.2 255.255.255.0
ScSwitch01(config-if)# standby 3 ip  10.239.66.1
ScSwitch01(config-if)# standby 3 priority 200
ScSwitch01(config-if)# standby 3 preempt
ScSwitch01(config-if)# standby 3 track fastEthernet 0/23 150
ScSwitch01(config-if)#interface vlan 4
ScSwitch01(config-if)# ip address 10.239.67.2 255.255.255.0
ScSwitch01(config-if)# standby 4 ip  10.239.67.1
ScSwitch01(config-if)# standby 4 priority 200
ScSwitch01(config-if)# standby 4 preempt
ScSwitch01(config-if)# standby 4 track fastEthernet 0/23 150
ScSwitch01(config-if)#interface vlan 5
ScSwitch01(config-if)# ip address 10.239.68.2 255.255.255.0
ScSwitch01(config-if)# standby 5 ip  10.239.68.1
ScSwitch01(config-if)# standby 5 priority 200
ScSwitch01(config-if)# standby 5 preempt
ScSwitch01(config-if)# standby 5 track fastEthernet 0/23 150
ScSwitch01(config-if)#interface vlan 6
ScSwitch01(config-if)# ip address 10.239.69.2 255.255.255.0
ScSwitch01(config-if)# standby 6 ip  10.239.69.1
ScSwitch01(config-if)# standby 6 priority 200
ScSwitch01(config-if)# standby 6 preempt
ScSwitch01(config-if)# standby 6 track fastEthernet 0/23 150
ScSwitch01(config-if)#interface vlan 7
ScSwitch01(config-if)# ip address 10.239.70.2 255.255.255.0
ScSwitch01(config-if)# standby 7 ip  10.239.70.1
ScSwitch01(config-if)# standby 7 priority 200
ScSwitch01(config-if)# standby 7 preempt
ScSwitch01(config-if)# standby 7 track fastEthernet 0/23 150
ScSwitch01(config-if)#interface vlan 8
ScSwitch01(config-if)# ip address 10.239.71.2 255.255.255.0
ScSwitch01(config-if)# standby 8 ip  10.239.71.1
ScSwitch01(config-if)# standby 8 priority 200
ScSwitch01(config-if)# standby 8 preempt
ScSwitch01(config-if)# standby 8 track fastEthernet 0/23 150
```

Figura 6-38 Configuración HSRP

6.3.8 Configuración SVI

Sintaxis de comandos IOS de Cisco – Configurar SVI		
1º	Modo configuración global	`Switch#configure terminal`
2º	Crear SVI por cada VLAN	`Switch(config)#interfaz vlan id`
3º	Asignar una dirección IP por cada SVI	`Switch(config-if)#ip address ip-address mask`

Tabla 6-32 Comandos para configurar SVI

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hos
Switch(config)#hostname ScSwitch01
ScSwitch01(config)#ip routing
ScSwitch01(config)#interface vlan 2
ScSwitch01(config-if)#ip address 10.239.65.2 255.255.255.0
ScSwitch01(config-if)#no shutdown
ScSwitch01(config-if)#exit
ScSwitch01(config)#interface vlan 3
ScSwitch01(config-if)#ip address 10.239.66.2 255.255.255.0
ScSwitch01(config-if)#no shutdown
ScSwitch01(config-if)#exit
ScSwitch01(config)#interface vlan 4
ScSwitch01(config-if)#ip address 10.239.67.2 255.255.255.0
ScSwitch01(config-if)#no shutdown
ScSwitch01(config-if)#exit
ScSwitch01(config)#interface vlan 5
ScSwitch01(config-if)#ip address 10.239.68.2 255.255.255.0
ScSwitch01(config-if)#no shutdown
ScSwitch01(config-if)#exit
ScSwitch01(config)#interface vlan 6
ScSwitch01(config-if)#ip address 10.239.69.2 255.255.255.0
ScSwitch01(config-if)#no shutdown
ScSwitch01(config-if)#exit
ScSwitch01(config)#interface vlan 7
ScSwitch01(config-if)#ip address 10.239.70.2 255.255.255.0
ScSwitch01(config-if)#shutdown
ScSwitch01(config-if)#exit
ScSwitch01(config)#interface vlan 8
ScSwitch01(config-if)#ip address 10.239.71.2 255.255.255.0
ScSwitch01(config-if)#no shutdown
ScSwitch01(config-if)#exit
ScSwitch01(config)#interface vlan 1
ScSwitch01(config-if)#shutdown
ScSwitch01(config-if)#end
ScSwitch01#
00:34:44: %SYS-5-CONFIG_I: Configured from console by console
ScSwitch01#wr
Building configuration...
[OK]
ScSwitch01#
```

Figura 6-39 Configuración SVI

6.3.9 Configuración RACL y VACL

Las VACL tienen un tratamiento especial, y los comandos de aplicación se detallan en la siguiente tabla. Sin embargo, las RACL se configuran del mismo modo que las ACL vistas anteriormente en el apartado 6.2.5.7.

Sintaxis de comandos IOS de Cisco – Configurar VACL		
1º	Modo configuración global	`Switch#configure terminal`
2º	Definir el mapa de acceso a la VLAN	`Switch(config)#vlan access-map nombre_map [secuencia]`
3º	Configurar la reglas	`Switch(config-access-map)#match ip address NOMBRE_ACL`
4º	Configurar la acción a tomar	`Switch(config-access-map)#action {drop | forward}`
5º	Aplicar el mapa de acceso a la VLAN	`Switch(config)#vlan filter nombre_map vlan-list VLAN`

Tabla 6-33 Comandos para configurar VACL

La Figura 6-40 ilustra como configurar una VACL en un switch de capa 3, de tal forma que impida el acceso de los usuarios a las páginas de administración de las impresoras, SAI y puentes inalámbricos, permitiéndolo solo desde la VLAN de informática. En este caso, se toma como ejemplo O'Donell.

```
ScSwitch01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch01(config)#ip access-list extended ACL_Odonell1
ScSwitch01(config-ext-nacl)#$0 0.0.0.255 10.239.69.200 0.0.0.7 eq 80
ScSwitch01(config-ext-nacl)#$0 0.0.0.255 10.239.69.200 0.0.0.7 eq 443
ScSwitch01(config-ext-nacl)#$0 0.0.0.255 10.239.69.208 0.0.0.15 eq 80
ScSwitch01(config-ext-nacl)#$0 0.0.0.255 10.239.69.208 0.0.0.15 eq 443
ScSwitch01(config-ext-nacl)#$0 0.0.0.255 10.239.69.224 0.0.0.31 eq 80
ScSwitch01(config-ext-nacl)#$0 0.0.0.255 10.239.69.224 0.0.0.31 eq 443
ScSwitch01(config-ext-nacl)#end
ScSwitch01#
000163: *Mar  1 02:21:42: %SYS-5-CONFIG_I: Configured from console by console
ScSwitch01#cont
ScSwitch01#conf
ScSwitch01#configure t
ScSwitch01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch01(config)#vlan access-map VACL_Odonell
ScSwitch01(config-access-map)#match ip address ACL_Odonell
ScSwitch01(config-access-map)#action drop
ScSwitch01(config-access-map)#vlan access-map VACL_Odonell
ScSwitch01(config-access-map)#action forward
ScSwitch01(config-access-map)#vlan filter VACL_Odonell vlan-list 6
ScSwitch01(config)#
ScSwitch01(config)#exit
ScSwitch01#show vla
000164: *Mar  1 02:22:17: %SYS-5-CONFIG_I: Configured from console by console
```

Figura 6-40 Restringir el acceso a las pag. de administración, SAI y puentes inalámbricos

Para garantizar el cumplimiento del requisito REQ_17, visto en el capítulo 4, según el cual el administrador debe asegurar que las VLANs de los usuarios no se vean entre sí, se crea la ACL mostrada en la Figura 6-41. En este caso, de nuevo se toma como ejemplo O'Donell.

```
ScSwitch01(config)#ip access-list extended ACL_Usuarios_Odonell
ScSwitch01(config-ext-nacl)# deny   ip 10.239.69.0 0.0.0.255 10.239.68.0 0.0.0.255
ScSwitch01(config-ext-nacl)# deny   ip 10.239.69.0 0.0.0.255 10.239.70.0 0.0.0.255
ScSwitch01(config-ext-nacl)# deny   ip 10.239.69.0 0.0.0.255 10.239.71.0 0.0.0.255
ScSwitch01(config-ext-nacl)#permit ip any any
```

Figura 6-41 Bloquear el tráfico procedente de otras VLANs de usuario

Para garantizar el cumplimiento del requisito REQ_16, según el cual el administrador debe asegurar que ningún usuario no autorizado accede por ssh a los servidores, se crea la primera de las ACLs extendida mostrada en la Figura 6-42.

Para garantizar el cumplimiento del requisito REQ_15, según el cual el administrador debe asegurar que ningún usuario no autorizado accede a la VLAN de administración, se crea la segunda de las ACLs extendida mostrada en la Figura 6-42.

```
ip access-list extended ACL_Servidores
 permit tcp 10.239.67.0 0.0.0.255 eq 22 10.239.65.0 0.0.0.255
 deny   tcp 10.239.67.0 0.0.0.255 eq 22 any
 permit ip any any
```

```
ip access-list extended ACL_Administracion
 permit ip 10.239.71.0 0.0.0.255 10.239.65.0 0.0.0.255
```

Figura 6-42 Creación de listas de acceso extendida

Por ultimo, la siguiente figura muestra los pasos para aplicar las ACL anteriores.

```
ScSwitch01(config)#interface vlan 6
ScSwitch01(config-if)#ip access-group ACL_Usuarios_Odonell in
ScSwitch01(config-if)#end
```

```
Switch01(config)#interface vlan 8
Switch01(config-if)#ip access-group  ACL_Administracion   in
Switch01(config-if)#end
```

```
ScSwitch01(config)#interface vlan 4
ScSwitch01(config-if)#ip access-group  ACL_Servidores  in
ScSwitch01(config-if)#end
```

Figura 6-43 Aplicación de las ACLs a la VLAN de O'Donell

6.3.10 Configuración del DHCP

Sintaxis de comandos IOS de Cisco – Configurar DHCP		
1º	Modo configuración global	`Switch#configure terminal`
2º	Configurar un pool de direcciones para cada VLAN	`Switch(config)# ip dhcp pool NOMBRE_POOL`
3º	Definir el segmento de red	`Switch(dhcp-config#network IP MASCARA`
4º	Definir el gateway	`Switch(dhcp-config)#default-router IP`
5º	Definir el servidor de DNS	`Switch(dhcp-config)#dns-server IP`
6º	Definir el sufijo de DNS	`Switch(dhcp-config)#domain-name dominio`
7º	Definir el tipo de petición de Netbios	`Switch(dhcp-config)# netbios-node-type h-node`
8º	Definir el servidor de WINS	`Switch(dhcp-config)# netbios-name-server IP`
9º	Definir el tiempo de arrendamiento de la IP	`Switch(dhcp-config)# lease infinite`

Tabla 6-34 Comandos para configurar DHCP

```
ScSwitch01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch01(config)#
ScSwitch01(config)#ip dhcp pool Informatica
ScSwitch01(dhcp-config)#   network 10.239.65.0 255.255.255.0
ScSwitch01(dhcp-config)#   default-router 10.239.65.1
ScSwitch01(dhcp-config)#   dns-server 10.239.67.106 10.160.4.66 10.253.2.160
ScSwitch01(dhcp-config)#   domain-name iaj.junta-andalucia.es
ScSwitch01(dhcp-config)#   netbios-name-server 10.239.67.107
ScSwitch01(dhcp-config)#   netbios-node-type h-node
ScSwitch01(dhcp-config)#   lease infinite
ScSwitch01(dhcp-config)#   exit
ScSwitch01(config)#
ScSwitch01(config)#
ScSwitch01(config)#ip dhcp pool Olive
ScSwitch01(dhcp-config)#   network 10.239.66.0 255.255.255.0
ScSwitch01(dhcp-config)#   default-router 10.239.66.1
ScSwitch01(dhcp-config)#   dns-server 10.239.67.106 10.160.4.66 10.253.2.160
ScSwitch01(dhcp-config)#   domain-name iaj.junta-andalucia.es
ScSwitch01(dhcp-config)#   netbios-name-server 10.239.67.107
ScSwitch01(dhcp-config)#   netbios-node-type h-node
ScSwitch01(dhcp-config)#   lease infinite
ScSwitch01(dhcp-config)#   exit
ScSwitch01(config)#
ScSwitch01(config)#ip dhcp pool Bilbao
ScSwitch01(dhcp-config)#   network 10.239.68.0 255.255.255.0
ScSwitch01(dhcp-config)#   default-router 10.239.68.1
ScSwitch01(dhcp-config)#   dns-server 10.239.67.106 10.160.4.66 10.253.2.160
ScSwitch01(dhcp-config)#   domain-name iaj.junta-andalucia.es
ScSwitch01(dhcp-config)#   netbios-name-server 10.239.67.107
ScSwitch01(dhcp-config)#   netbios-node-type h-node
ScSwitch01(dhcp-config)#   lease infinite
ScSwitch01(dhcp-config)#   exit
ScSwitch01(config)#
ScSwitch01(config)#ip dhcp pool Odonell
ScSwitch01(dhcp-config)#   network 10.239.69.0 255.255.255.0
ScSwitch01(dhcp-config)#   default-router 10.239.69.1
ScSwitch01(dhcp-config)#   dns-server 10.239.67.106 10.160.4.66 10.253.2.160
ScSwitch01(dhcp-config)#   domain-name iaj.junta-andalucia.es
ScSwitch01(dhcp-config)#   netbios-name-server 10.239.67.107
ScSwitch01(dhcp-config)#   netbios-node-type h-node
ScSwitch01(dhcp-config)#   lease infinite
ScSwitch01(dhcp-config)#   exit
ScSwitch01(config)#
```

Figura 6-44 Configuración DHCP

6.3.10.1 Reserva de IP por MAC

Sintaxis de comandos IOS de Cisco – Configurar reserva de IP por MAC		
1º	Modo configuración global	`Switch#configure terminal`
2º	Configurar un pool para el equipo	`Switch(config)# ip dhcp pool NOMBRE_EQUIPO`
3º	Definir la IP del host	`Switch(dhcp-config#host IP MASCARA`
4º	Definir la MAC para el host	`Switch(dhcp-config#client-identifier MAC`

Tabla 6-35 Comandos para configurar reserva IP por MAC

```
ScSwitch01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch01(config)#ip dhcp pool SSCC004
ScSwitch01(dhcp-config)#   host 10.239.66.4 255.255.255.0
ScSwitch01(dhcp-config)#   client-identifier 0100.3005.7f00.35
ScSwitch01(dhcp-config)#end
```

Figura 6-45 Configuración reserva IP por MAC

6.3.10.2 Excluir rangos de IP en el DHCP

Sintaxis de comandos IOS de Cisco – Configurar la exclusión de direcciones IP		
1º	Modo configuración global	`Switch#configure terminal`
2º	Excluir rango de IP	`Switch(config)# ip dhcp excluded-address IP_baja IP_alta`

Tabla 6-36 Comandos para configurar reserva IP por MAC

```
ScSwitch01(config)#
ScSwitch01(config)#ip dhcp excluded-address 10.239.70.0 10.239.70.255
ScSwitch01(config)#ip dhcp excluded-address 10.239.69.0 10.239.69.255
ScSwitch01(config)#ip dhcp excluded-address 10.239.68.0 10.239.68.255
ScSwitch01(config)#ip dhcp excluded-address 10.239.66.0 10.239.66.255
ScSwitch01(config)#ip dhcp excluded-address 10.239.65.0 10.239.65.255
ScSwitch01(config)#end
```

Figura 6-46 Excluir rangos de ip en el DHCP

6.3.10.3 Configuración DHCP Snooping en un switch de capa 3

Tanto para los switches de capa 2 como para los de capa 3, los comandos para configurar DHCP Snooping son los mismos, y se trataron se trataron en la Tabla 6-17 del presente capitulo. En aquel momento se describieron los pasos para la configuración de un switch de capa 2, ScSwitch12, y en esta ocasión la siguiente figura muestra el proceso para un switch de capa 3, ScSwitch01.

```
ScSwitch01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch01(config)#ip dhcp snooping
ScSwitch01(config)#ip dhcp snooping information option
ScSwitch01(config)#interface range gigabitEthernet 0/7 - 9, gigabitEthernet 0/24
ScSwitch01(config-if-range)#ip dhcp snooping trust
ScSwitch01(config-if-range)#exit
ScSwitch01(config)#ip dhcp snooping vlan 2 3
ScSwitch01(config)#ip dhcp snooping vlan 5 6
ScSwitch01(config)#end
ScSwitch01#
```

Figura 6-47 Configuración DHCP Snooping en un switch de capa 3

6.3.11 Configuración de DAI

Sintaxis de comandos IOS de Cisco – Configurar DAI		
1º	Modo configuración global	`Switch#configure terminal`
2º	Configuración interfaces confiables	`Switch(config)# interface fastethernet 0/X` `Switch(config-if)# ip arp inspection trust`

3º	Habilitar DAI	`Switch(config)#ip arp inspection vlan X`
		`Switch(config)# ip arp inspection validate src-mac dst-mac ip`
		`Switch(config)# ip arp inspection log-buffer entries 1024`

Tabla 6-37 Comandos para configurar DAI

```
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch01(config)#ip arp inspection vlan 3,5,6
ScSwitch01(config)#ip arp inspection validate src-mac dst-mac ip
ScSwitch01(config)#ip arp inspection log-buffer entries 1024
ScSwitch01(config)#
```

Figura 6-48 Configuración DHCP Snooping en un switch de capa 3

6.3.12 Configuración de las interfaces

6.3.12.1 Configuración de Etherchannel

Sintaxis de comandos IOS de Cisco – Configurar Etherchannel		
1º	Modo configuración global	`Switch#configure terminal`
2º	Especificar las interfaces que formaran parte del grupo de Etherchannel	`Switch(config)# interface range fastethernet [rango_interfaz]`
3º	Crear la interfaz port-channel	`Switch(config-if-range)#channel-group N mode desirable`

4º	Crear el enlace troncal en la interfaz de port-channel	`Switch(config)#interface port-channel N` `Switch(config-if)#switchport mode trunk`

Tabla 6-38 Comandos para configurar Etherchannel

```
ScSwitch01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch01(config)#interface range gigabitEthernet 0/1 - 2
ScSwitch01(config-if-range)#switchport trunk encapsulation dot1q
ScSwitch01(config-if-range)#switchport mode trunk
ScSwitch01(config-if-range)#channel-group 1 mode desirable
ScSwitch01(config-if-range)#interface port-channel 1
ScSwitch01(config-if)#switchport mode trunk
ScSwitch01(config-if)#end
ScSwitch01#
ScSwitch01#
```

Figura 6-49 Configuración de Etherchannel

6.3.12.2 Configuración de puertos SPAN

Para poder monitorizar el tráfico de entrada y salida de la red, son necesarios los puertos Span. A un puerto Span se le conoce como “analizador de puerto conmutado”, “reflector de puerto” o “monitor de puertos”. Básicamente se trata de un puerto del switch destinado a labores especiales, ya que el administrador de red lo configura para que refleje el tráfico recibido en otros puertos.

De este modo, el tráfico que va entre el switch y el router, o entre el switch y el cortafuego, se puede copiar en el puerto SPAN al que está conectado el servidor de gestión de la red. Persiguiendo este objetivo, en el switch principal de la red del IATE se ha reservado un puerto para que funcione como Span.

Sintaxis de comandos IOS de Cisco – Configurar puertos SPAM		
1º	Modo configuración global	`Switch#configure terminal`
2º	Definir una sesión de monitorización, definiendo la interfaz origen	`Switch(config)# monitor session N source interface fastethernet 0/X`
3º	Definir la interfaz de destino que va recibir todo el trafico monitorizado	`Switch(config)#monitor session N destination interface fastethernet 0/Y`

Tabla 6-39 Comandos para configurar puertos SPAN

```
ScSwitch01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch01(config)#monitor session 1 source interface gigabitEthernet 0/23
ScSwitch01(config)#$sion 1 destination interface gigabitEthernet 0/22
ScSwitch01(config)#
ScSwitch01(config)#
ScSwitch01(config)#end
```

Figura 6-50 Configuración puerto Span

6.4 Configuración de los puentes inalámbricos

Los pasos expuestos a continuación son de aplicación a cada uno de los puentes inalámbricos.

- **Paso 1**. Establecer el nombre del puente y la dirección IP estática.

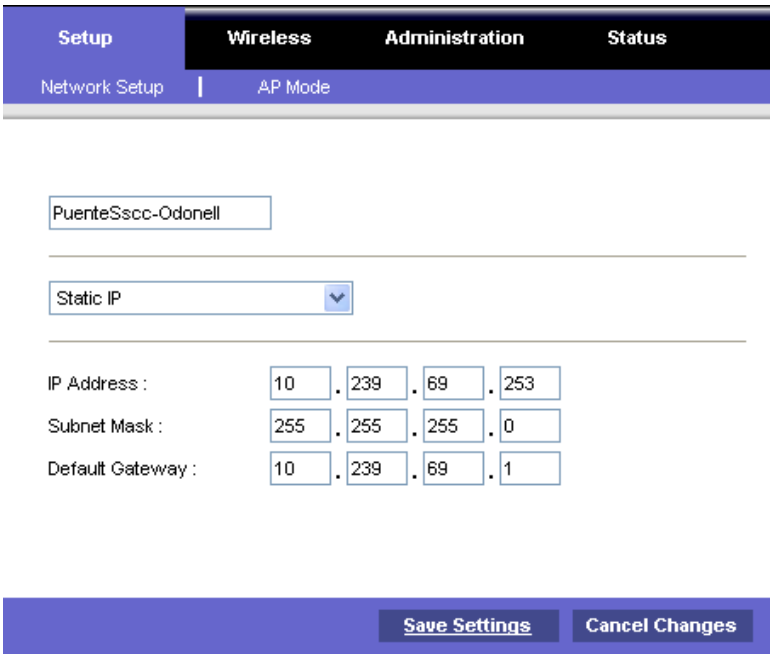


Figura 6-51 Paso 1. Opción Network Setup

- **Paso 2**. Establecer el SSID y deshabilitar la difusión para que el SSID quede oculto.

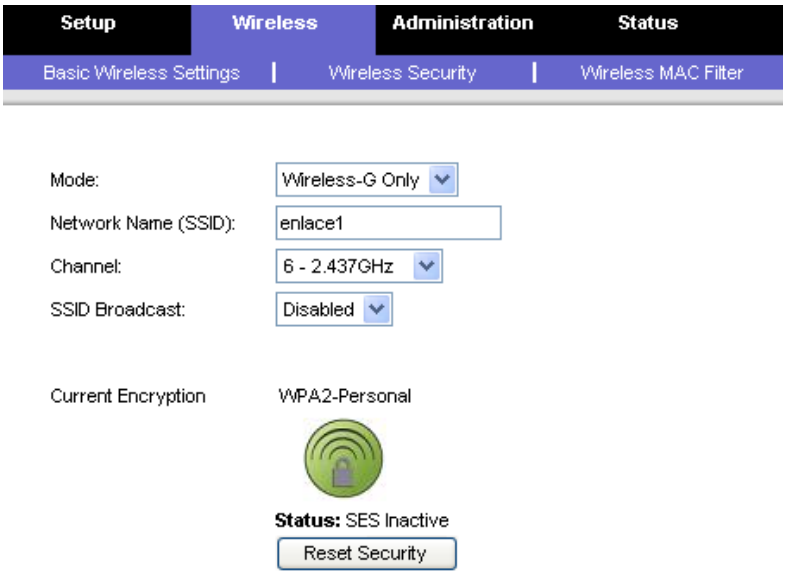


Figura 6-52 Paso 2. Opción Basic Wireless Settings

- **Paso 3**. Establecer seguridad WPA2 en el puente, que incorpora estándares de encriptación y seguridad avanzados (AES).

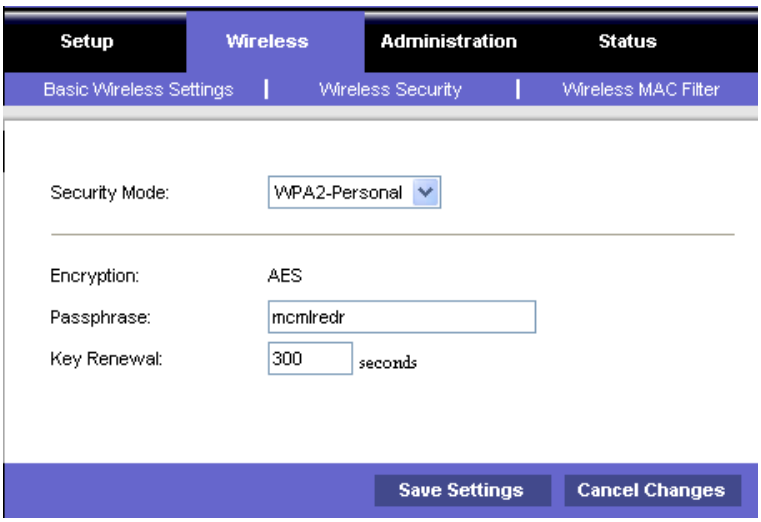


Figura 6-53 Paso 3. Opción Wireless Security

- **Paso 4**. Establecer el modo Bridge, para permitir crear un enlace punto a punto entre los dos edificios. La asociación se realiza insertando la MAC del puente al que se va asociar, en este caso al de O'Donell.

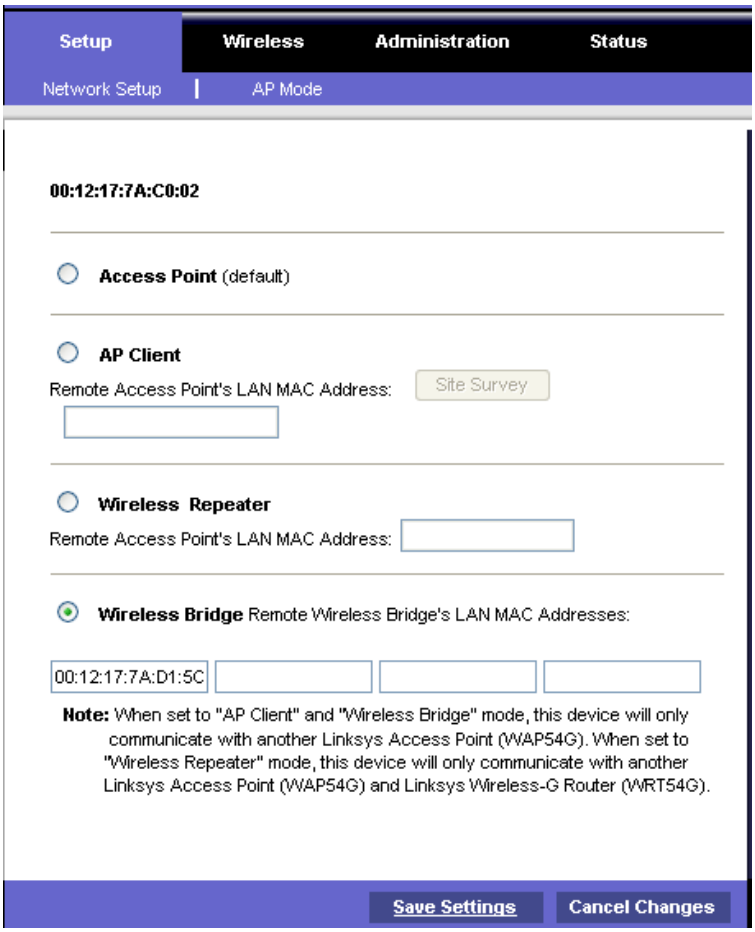


Figura 6-54 Paso 4. Opción AP Mode

- **Paso 5**. Activar el envío de log al servidor de syslog.

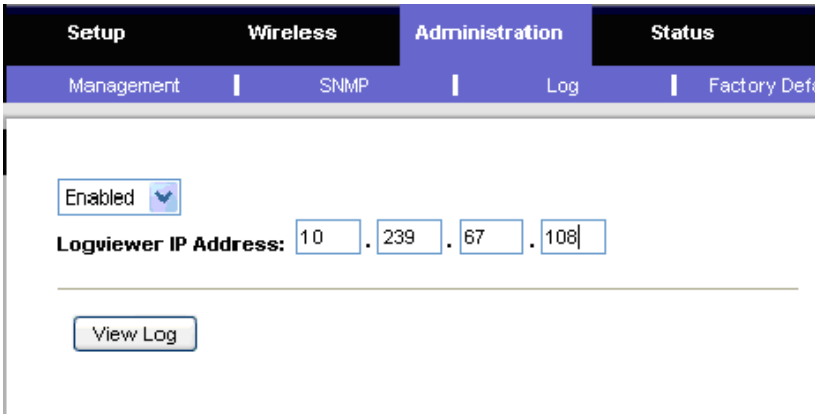


Figura 6-55 Paso 5. Opción Log

6.5 Mantenimiento

La capacidad de respaldo y restauración de la configuración son habilidades fundamentales para administrar un switch. Este apartado detalla el procedimiento que se ha seguido para mantener la configuración de la electrónica de red y de los puentes inalámbricos de la red del IATE.

6.5.1 Configuraciones de respaldo y restauración de la configuración del switch

Una tarea típica del técnico de red es la de cargar al switch una configuración. En este punto se explica cómo cargar y almacenar la configuración del switch en un servidor TFTP (Trivial file transfer Protocol o Protocolo de transferencia de archivos trivial).

Una vez configurado el switch con todas las opciones deseadas, es recomendable hacer una copia de seguridad de la configuración y colocarla en un archivo junto con las copias de seguridad del resto de la información de la red. Al tener la configuración almacenada de manera segura fuera del switch, éste queda protegido en caso de que surja algún problema serio.

Si se pierde la configuración debido a un fallo en el hardware del switch, habrá que configurarlo otra vez. Si existe una copia de seguridad de la configuración del switch fallido, ésta puede cargarse rápidamente en el switch, sin necesidad de configurarlo de nuevo desde cero.

Se puede utilizar TFTP para realizar la copia de seguridad de los archivos de configuración en la red. El software IOS de Cisco viene con un cliente de TFTP incorporado que permite que el

administrador se conecte con un servidor TFTP en su red. Para almacenar un archivo de configuración del switch en el servidor TFTP, se deben seguir los siguientes pasos:

- **Paso 1**. Verificar que el servidor TFTP se está ejecutando en la red.

- **Paso 2**. Iniciar sesión en el switch a través del puerto de consola o sesión SSH. Habilitar el switch y luego hacer ping al servidor TFTP.

- **Paso 3**. Subir la configuración del switch al servidor TFTP. Para ello, especificar la dirección IP o el nombre de host del servidor TFTP y el nombre del archivo de destino. El comando del IOS de Cisco es:

  #copy system:running-config tftp:[[[//ubicación]/directorio]/nombre de archivo] ó
  #copy nvram:startup-config tftp:[[[//ubicación]/directorio]/nombre de archivo].

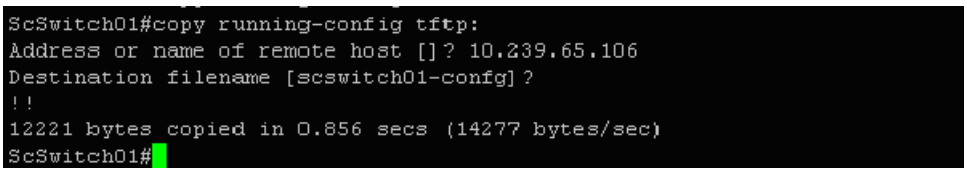


Figura 6-56 Copia de seguridad de la configuración en servidor TFTP

Una vez que la configuración se ha almacenado correctamente en el servidor TFTP, cuando sea necesario restaurarla en el switch los pasos a seguir son:

- **Paso 1.** Verificar que el servidor TFTP se está ejecutando en la red.

- **Paso 2.** Iniciar sesión en el switch a través del puerto de consola o sesión Telnet. Habilitar el switch y luego hacer ping al servidor TFTP.

- **Paso 3.** Descargar el archivo de configuración del servidor TFTP para configurar el switch. Para ello, especificar la dirección IP o el nombre de host del servidor TFTP y el nombre del archivo que desea descargar. El comando del IOS de Cisco es:

  #copy tftp:[[[//ubicación]/directorio]/nombre de archivo] system:running-config ó
  #copy tftp:[[[//ubicación]/directorio]/nombre de archivo] nvram:startup-config.

Para automatizar este proceso en el IATE, se han implementado los scripts Backup.sh y BackupSwitch.sh, y es necesario el fichero Listado_switch.dat, que contiene el listado de IPs de los switches. El segundo de ellos, como se puede ver a continuación, almacena la copia de seguridad del switch en el servidor TFTP, mientras que el script Backup.sh le pasa como parámetro los datos necesarios para realizar el backup del switch que está procesando, tales como IP del switch, usuario, contraseña, contraseña enable e IP del servidor TFTP. Al mismo tiempo, el script Backup.sh genera un fichero de log en el directorio /var/log/backup.

Aplicaciones Lugares Sistema

root@ingenia:/usr/local/bin

Archivo Editar Ver Terminal Solapas Ayuda

```
#!/bin/bash

FICH=listado_switch
USO="Uso: backup usuario password password_enable ip_tftp"
#
# Fecha Y Hora
#
hoy=`date +%Y%m%d`
LOG="/var/log/backup/"$hoy".chk"

if [ $# -ne 4 ]; then
echo $USO
exit
fi

  echo -e "*********************************************\n" >> $LOG
  echo -e "Comienzo del backup de los switch del IATE\n " >> $LOG
  echo -e "*********************************************\n" >> $LOG
while read SWITCH
do
 SSH=$1@$SWITCH
 BackupSwitch.sh $SSH $2 $3 $4
 if [ $? -eq 0 ]; then
  echo -e "Se ha procesado el switch $SWITCH\n" >> $LOG
 else
  echo -e "ERROR EN EL BACKUP DEL SWITCH $SWITCH\n" >> $LOG
 fi
done < $FICH

  echo -e "*********************************************\n" >> $LOG
  echo -e "FIN DEL BACKUP \n " >> $LOG
  echo -e "*********************************************\n" >> $LOG

backup.sh (END)
```

root@ingenia:/usr/local/bin

Figura 6-57 Script Backup.sh

```
#!/usr/bin/expect -f

 set timeout -1
 match_max 100000
 eval spawn "ssh [lindex $argv 0]"

 expect  "*assword: "
 send -- "[lindex $argv 1]\r"
 expect  "*>"
 send -- "en\r"
 expect  "*assword: "
 send -- "[lindex $argv 2]\r"
 expect  "*#"
 send -- "copy running-config tftp:\r"
 expect  "*? "
 send -- "[lindex $argv 3]\r"
 expect  "*? "
 send -- "\r"
 expect  "*copied*#"
 send -- "q\r"
BackupSwitch.sh (END)
```

root@ingenia:/usr/local/bin

Figura 6-58 Script BackupSwitch.sh

6.5.2 Backup de la configuración de los puentes inalámbricos

En el caso de los puentes inalámbricos el procedimiento es muy sencillo, ya que el menú de administración dispone de la opción “Backup File”, por lo que simplemente hay que indicar donde se desea guardar el fichero.

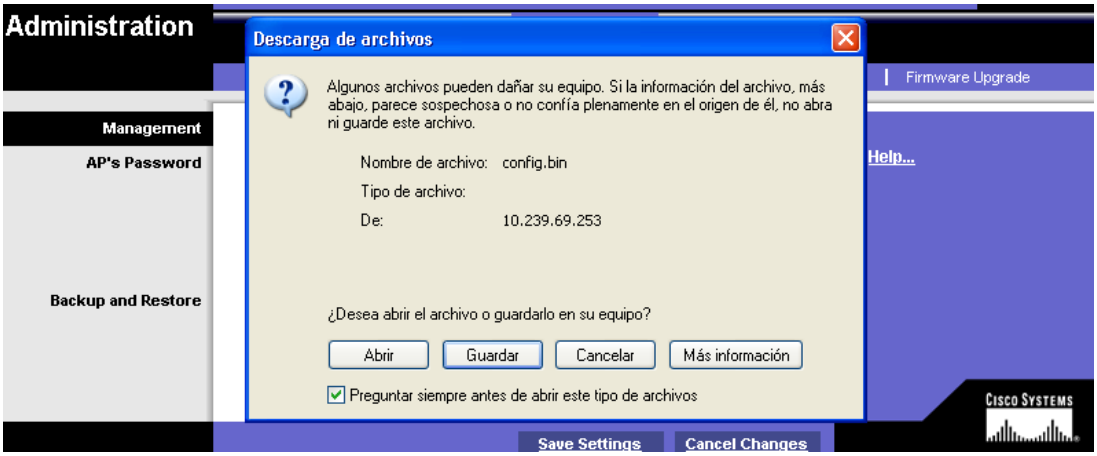


Figura 6-59 Backup de la configuración del puente inalámbrico

6.6 Conclusiones

A lo largo del capítulo se ha mostrado la sintaxis de los comandos que permiten configurar la electrónica de red de acuerdo a lo expuesto durante el diseño de la LAN, así como implementar las medidas de seguridad descritas en el capítulo 4. A modo de ejemplo, para cada uno de los casos se ha aportado la salida por consola obtenida durante la ejecución del proceso en los switches ScSwitch12 y ScSwitch01 de la red IATE.

Por otra parte, también se han mostrados los pasos para la configuración de los puentes inalámbricos, necesarios para llevar a cabo el despliegue de la WLAN. Finalmente, se ha descrito el procedimiento seguido para realizar el backup de la configuración de los switches, así como de la configuración de los puentes inalámbricos, con el fin de agilizar el proceso de configuración si fuese necesario restaurarla.

Con todo esto, se cierra uno de los bloques principales de este proyecto fin de carrera, ya que de acuerdo al plan de actuación expuesto en el capítulo 2, se han concluido 3 de las 5 fases en las que se dividió el proyecto, Estudios Previos, Diseño, e Instalación, y prácticamente también la cuarta de las fases, Configuración. No obstante, el broche final a esta última será puesto en el siguiente capitulo, donde se trata la configuración de las herramientas dedicadas a la gestión de red.

Capítulo 7.
Gestión de la red

7.1 Introducción

Los principales objetivos de la gestión de red son reducir la indisponibilidad de la red, disminuir los costes de operación, y obtener un rendimiento óptimo de la red para poder aprovechar sus recursos al máximo. Esto se consigue dedicando esfuerzos a tres tareas fundamentales, como son, controlar la disponibilidad de los dispositivos revisando su estado a través de logs, controlar la CPU del switch más poderoso con el fin de garantizar que soporta toda la carga de la red, y monitorizar los cuellos de botella y la lentitud en la red provocada por la saturación del ancho de banda. A esto se une una actividad adicional que contribuye a que los técnicos puedan desempeñar su trabajo con mayor facilidad, y que consiste en que el administrador mantenga la documentación de red debidamente actualizada y en un lugar seguro.

La gestión de la red está recomendada no sólo en grandes empresas, sino también en redes pequeñas, ya que además de reducir el tiempo de respuesta ante la caída del sistema, ayuda a identificar problemas con la anticipación suficiente como para evitar que la situación se convierta en una emergencia.

Dada su importancia y teniendo en cuenta que, como se apuntó en el capitulo 2, la falta de gestión de la red fue una de las principales carencias detectadas durante el análisis previo realizado al IATE, se hacía imprescindible incluir una sección dedicada a este tema.

En el IATE los objetivos descritos anteriormente se alcanzan utilizando SNMP, Syslog, un par de herramientas complementarias llamadas Nagios y Cacti, las cuales hacen uso de SNMP y sirven para controlar los eventos que ocurran en la red , y mediante la implantación del control de configuración en la documentación de red. En este capitulo se ilustra también la arquitectura lógica y física de la infraestructura de gestión de red implantada en el IATE.

7.2 SNMP

En general, como refleja la Figura 7-1, la arquitectura lógica para la gestión de una red de Telecomunicaciones se compone de los siguientes elementos.

- Al menos un servidor de gestión de la red o NMS (Network Management System), donde se reciben los mensajes de la red, entre los que se incluyen alertas y datos de interés, que permiten al administrador controlar el estado de la red. El servidor de monitorización del IATE está ubicado en el CPD de SS.CC., en la VLAN de servidores, como se puede observar en la Figura 7-2, y tiene las siguientes características.
    - Fujitsu Siemens Primergy RX220
    - 2 x Disco duro 150 Gb
    - Raid 0
    - 1Gb de Ram
    - Procesador 64-bits AMD Opteron 2,2 GHz
    - 3 tarjetas de red (Una para administración, otra para las herramientas de gestión de red, y una tercera para el NTop)

- Dispositivos de red en los que existe un proceso o agente que se encarga de comunicar dicho equipo con el servidor de gestión de la red.

- Un protocolo de gestión, encargado de transportar hasta el servidor la información del equipo proporcionada por el agente. En el presente proyecto se ha empleado el Protocolo de Gestión de Red Simple, basado en TCP/IP, y también conocido como SNMP (Simple Network Management Protocol).

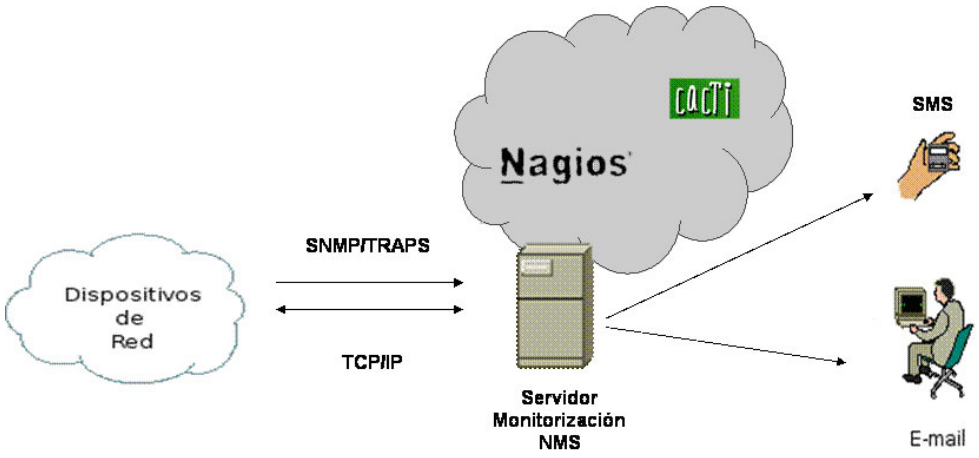


Figura 7-1 Gestión de la red.

De todos los dispositivos que forman parte de la arquitectura física, solo se controlan los que se consideran críticos, es decir, aquellos que en caso de fallo o perdida de conectividad provocan la perdida de servicio. Entre estos elementos se encuentran los routers, switches, puntos de acceso y puentes inalámbricos. En la Figura 7-2 se han marcado en rojo los puntos que se consideran objeto de monitorización con el fin de controlar el tráfico que soporta la red del IATE.

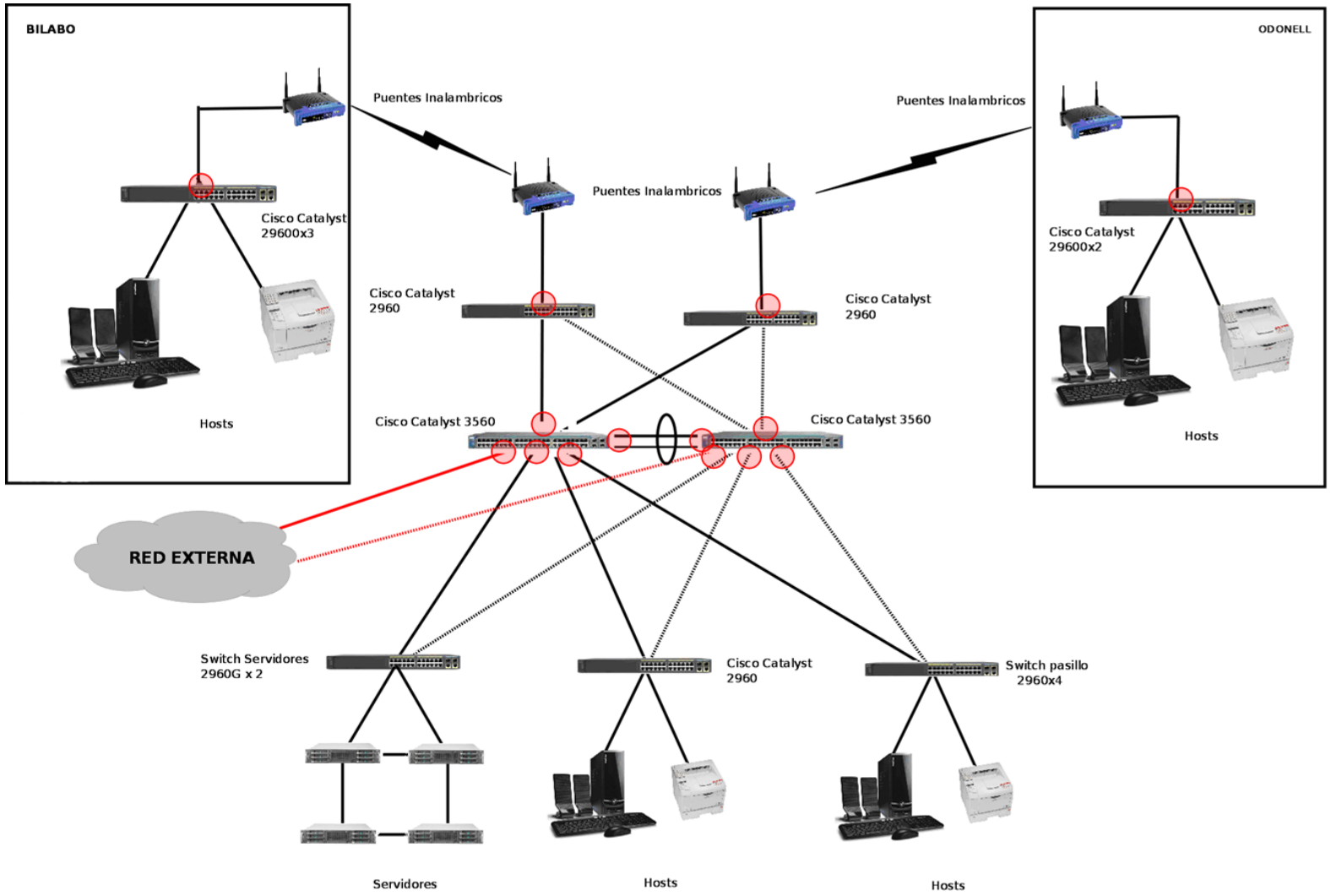


Figura 7-2 Gestión de la red. Arquitectura Física

SNMP es un protocolo de administración de red que permite que los administradores recopilen datos sobre la red y los dispositivos correspondientes. Se trata de un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre los dispositivos de red y puede emplearse para administrar routers, switches, puntos de acceso inalámbricos, firewall o cualquier otro dispositivo capaz de soportarlo.

SNMP permite a los administradores de red gestionar el rendimiento de la misma, así como localizar y resolver problemas en ella, y planificar su crecimiento.

El software del sistema de administración SNMP se encuentra disponible en herramientas como CiscoWorks, Nagios o Cacti, mientras que el software del agente de administración SNMP suele estar incorporado en los sistemas operativos de servidores, routers y switches.

SNMP tiene cuatro componentes principales:

- Estación de administración. Es un PC con la aplicación de administración SNMP cargada, utilizado por el administrador para gestionar y configurar la red.
- Agente de administración, que no es más que software instalado en un dispositivo administrado por SNMP.
- Base de información de administración (MIB o Management Information Base), que es la base de datos que un dispositivo mantiene sobre sí mismo en relación con los parámetros de rendimiento de la red.
- Protocolo de administración de red o protocolo de comunicación utilizado entre la estación de administración y el agente de administración.

Los agentes también se pueden configurar con Trap. Una Trap es un evento que acciona una alarma. Ciertas áreas del agente se configuran con umbrales que deben mantenerse, tales como la cantidad de tráfico al que un puerto específico puede acceder. Si se supera el umbral, el agente envía un mensaje de alerta a la estación de administración. Los Traps evitan que la estación de administración necesite realizar sondeos continuos en los dispositivos de red.

7.2.1 Paquetes a instalar

La paquetería ha sido instalada vía yum install. Los paquetes necesarios para SNMP son:

- ✓ net-snmp-devel-5.3.2.2-7.el5_4.2
- ✓ net-snmp-utils-5.3.2.2-7.el5_4.2

- ✓ net-snmp-perl-5.3.2.2-7.el5_4.2
- ✓ net-snmp-libs-5.3.2.2-7.el5_4.2
- ✓ php-snmp-5.1.6-24.el5_4.5
- ✓ net-snmp-5.3.2.2-7.el5_4.2
- ✓ Para la gestión de Traps hay que compilar las fuentes snmptt_1.3 y perl-5.8.9

Además es necesario descargar las MIB utilizadas por los Switch Cisco para snmptt. Se pueden obtener de la página:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Por otra parte, el paquete net-snmp incluye la utilidad snmppconvertmib, que se utiliza para automatizar la creación de configuraciones snmptt a partir de un archivo MIB.

Por ultimo, se ha integrado con Nagios para capturar las Traps. El siguiente esquema resume el proceso seguido en el tratamiento de los Traps.

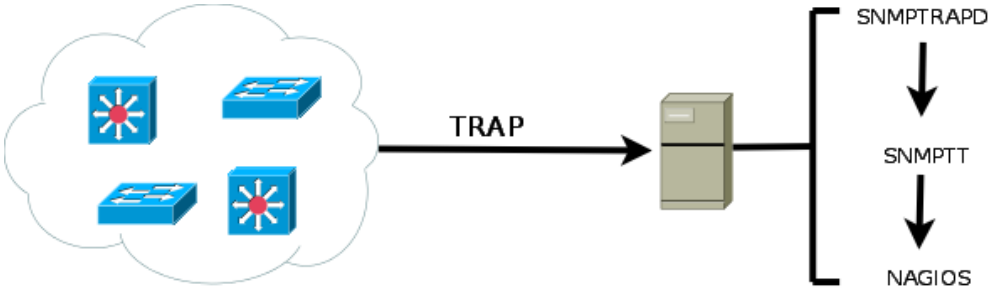


Figura 7-3 Integración SNMP y Nagios para la gestión de Traps

7.2.2 Ficheros de configuración

snmpd.conf	En este fichero se configuran las cadenas de conexión SNMP en función de la version SNMP (SNMP v1, SNMP v2c o SNMP v3)
Snmptrapd.conf	Es un demonio incluido en el paquete Net-SNMP, que sirve para configurar las comunidades SNMP y para configurar quien va a gestionar las Traps.
Snmptt.conf **Snmptt.ini**	Snmptt (SNMP Trap Translator) se encarga de tranformar la Trap recibida a un formato legible para el usuario. Se integra con snmptrapd y permite manipular los traps con más flexibilidad, ya que ciertos traps pueden ser capturados por snmptt y redirigidos a otro software, como por ejemplo Nagios (Ver Figura 7-3) Snmp.ini es el fichero de inicialización de snmptt.

Tabla 7-1 SNMP. Ficheros de configuración más significativos

7.2.3 Configuración del SNMP

Se deben realizar tres pasos para configurar SNMPv3:

1. Configurar los grupos SNMP para agrupar usuarios.
2. Configurar los usuarios SNMP, definiendo los nombres de usuario que residen en los hosts que se conectan al agente local.
3. Configurar los hosts SNMP para especificar el destinatario de una operación de notificación.

Sintaxis de comandos IOS de Cisco – Configurar SNMP		
1º	Modo configuración global	`Switch#configure terminal`
2º	Configuración de los grupos SNMP	`Switch(config)#snmp-server group name { v1 | v2c | v3 {auth | noauth | priv } } [read readview] [write writeview] [notify notifyview] [access access-list]`
3º	Configuración de Usuarios	`Switch(config)#snmp-server user username gruopname {v1 | v2c | v3 [auth {md5 | sha} auth-password [priv des56 priv-password]]} [access access-list]`
4º	Configuración del host SNMP	`Switch(config)#snmp-server host host-address [trap | informs] [version {1 | 2c | 3 [auth | noauth | priv ]}] community-string [udp-port port] [notification-type]`

Tabla 7-2 Configuración de SNMP

```
ScSwitch12#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch12(config)#snmp-server group cactigroup v3 priv
ScSwitch12(config)#$igroup v3 auth md5 mcmlredr priv des56 iateylmqlp
ScSwitch12(config)#$ host 10.239.67.108 traps version 3 priv cactiuser
ScSwitch12(config)#end
ScSwitch12#
00:32:08: %SYS-5-CONFIG_I: Configured from console by tecnico on console
ScSwitch12#
```

Figura 7-4 Configuración SNMP v3

```
ScSwitch12#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ScSwitch12(config)#snmp-server community 4c3s0 ro 1
ScSwitch12(config)#snmp-server enable traps
ScSwitch12(config)#snmp-server host 10.239.67.108 version 2c 4c3s0
ScSwitch12(config)#
```

Figura 7-5 Configuración SNMP v2

7.3 Revisión del estado de los dispositivos. Syslog

El protocolo syslog proporciona a una maquina un medio de transporte para que envíe mensajes de notificación de eventos, a través de redes IP, a un recolector de mensajes de eventos, también conocido como servidor syslog. Hay que destacar que uno de los principios fundamentales del protocolo syslog y de sus procesos es su simplicidad.

Para una instalación completa es necesaria la configuración tanto de la electrónica de red Cisco, que actuará como cliente, como del servidor Syslog. Los pasos para llevar a cabo la primera de las tareas se trataron en el capitulo 6 del presente proyecto, mientras que la configuración requerida en el servidor se describe a continuación.

7.3.1 Paquetes a instalar

No es necesario instalar ninguna paquetería adicional, ya que está incluida en la instalación del sistema operativo.

7.3.2 Ficheros de configuración

La Tabla 7-3 destaca los ficheros de configuración más relevantes para el Syslog. Una vez terminada la configuración será necesario reiniciar el servicio (/etc/init.d/syslog restart)

syslog	Situado en /etc/sysconfig/syslog. En este fichero de configuración se le indica al demonio de Syslog que escuche los mensajes de dispositivos remotos, mediante la variable que define las opciones para Syslog. SYSLOGD_OPTIONS="-m 0 -r -x" Opciones: -m 0: Deshabilita las marcas “MARK” en el mensaje de Syslog. -r: Habilita la recepción de log de maquinas remotas -x: Deshabilita la resolución de nombre de DNS recibidas con -r
Sylog.conf	Situado en /etc/syslog.conf. Este fichero especifica como tratar la información de logs, controla los mensajes que se muestran y donde se muestran. Cada entrada está definida por los campos facility, nivel y acción. Los dos últimos separados por una tabulación. ▪ Campo Facility. Indica el programa que genera los logs. Puede tomar uno

	de los siguientes valores. auth – Sistema de autenticación cron – Cron y at daemon – Demonios del sistema kern – Mensajes generados por el kernel lpr – Mensajes de impresión mail – Mensajes de mail user – Aplicaciones de usuario local0-local7 – Reservado para uso local syslog – Mensajes del demonio de syslog ▪ Campo Nivel. Indica el nivel de criticidad del log. Puede tomar uno de los siguientes valores. 0 - Emergency (emerg) 1 - Alerts (alert) 2 - Critical (crit) 3 - Errors (err) 4 - Warnings (warn) 5 - Notification (notice) 6 - Information (info) 7 - Debug (debug) **NOTA**: Se permiten el uso de comodines, tales como, *(representa todas las aplicaciones o todos los niveles), = (delante de un nivel indica que sólo se traten los mensajes de ese nivel), ! (delante de un nivel indica que se traten todos los niveles menos el especificado) ▪ Campo Acción. Indica como actuar ante la recepción del log. Habitualmente este campo determina el fichero de texto al que se desea almacenar los logs. En este fichero de configuración definir las siguientes entradas: local7.* /var/log/cisco/cisco.log local3.* /var/log/ntop/ntop.log

Tabla 7-3 Syslog. Ficheros de configuración más significativos.

Para automatizar el proceso de revisión de los logs y facilitar así el trabajo del administrador de la red, en el IATE se ha implementado un script de chequeo cuya función es monitorizar los log del sistema.

El script llamado ChequeaLog.sh es lanzado desde el cron cada 10 minutos. Su código fuente se proporciona en el DVD junto con el resto de documentación del proyecto, básicamente lo que hace es determinar la hora en ese instante de su ejecución y restarle 10 minutos (teniendo en cuenta cambios de día, mes, año e incluso años bisiestos), filtrar los logs producidos en ese rango horario y volcarlos a un fichero temporal, sobre el cual realiza un barrido con el comando "awk" para extraer qué switches están presentes en esos logs. Por cada switch inspecciona el número de evento producidos y su nivel de criticidad. Finalmente toda esta información se almacena en un fichero llamado Registro-AÑOMESDIA_HORAMINUTOS.log, que es enviado adjunto a la dirección del administrador de red.

La siguiente figura muestra un ejemplo de la salida de este script para el switch ScSwitch01

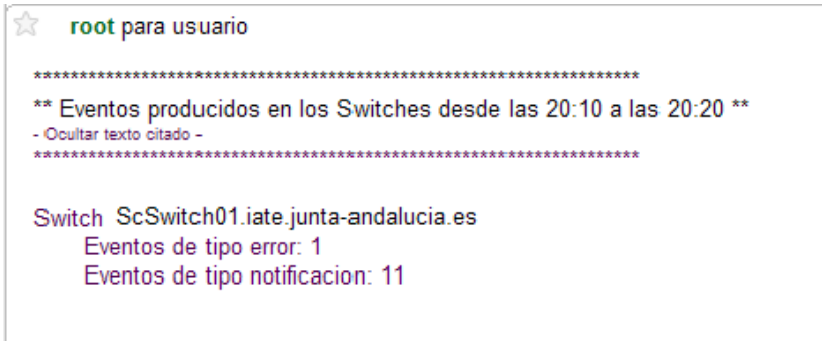


Figura 7-6 Notificación producida por el script ChequeaLog.sh

7.4 Herramientas para la gestión de la red.

Bajo esta sección se engloban las herramientas de código abierto implantadas en el IATE para la gestión de la red, tales como:

- Nagios
- Cacti
- Subversión (Apoyo a la gestión de red)

Se han escogido por su amplio uso en el mercado y evidentemente por aportar todas las ventanas del software libre, como pueden ser:

- Disminuir la dependencia con vendedores de código propietario, por ejemplo a la hora de requerir actualizaciones del producto, ya que a la larga supone un gasto de dinero y tiempo vital.

- Reducir costes, ya que no es necesario pagar por obtener licencias ni coste de mantenimiento. El bajo o nulo coste de los productos libres permite a las empresas ampliar sus infraestructuras sin que se vean mermados sus intentos de crecimiento por no poder hacer frente al pago de grandes cantidades en licencias.

- Libertad de uso y redistribución. Posibilidad de probar varias alternativas antes de decantarse por una de ellas. No todas las empresas propietarias ofrecen versiones de evaluación, mientras que las licencias de software libre permiten la instalación del software tantas veces y en tantas máquinas como el usuario desee.

- Soporte por parte de una comunidad de usuarios y amplia documentación en Internet.

- Ausencia de características inútiles, ya que las nuevas funcionalidades suelen venir dadas por las necesidades de los usuarios y no por las ideas de un departamento de desarrollo o marketing.

- Sistemas sin puertas traseras y más seguros. El acceso al código fuente permite que tanto hackers como empresas de seguridad de todo el mundo puedan auditar los programas, por lo que la existencia de puertas traseras es ilógica, ya que se pondría en evidencia y contraviene el interés de la comunidad que es la que lo genera.

- Corrección más rápida y eficiente de fallos. El funcionamiento e interés conjunto de la comunidad ha demostrado solucionar más rápidamente los fallos de seguridad en el software libre, algo que desgraciadamente en el software propietario es más difícil y costoso. Cuando se notifica a las empresas propietarias del software, éstas niegan inicialmente la existencia de dichos fallos por cuestiones de imagen y cuando finalmente admiten la existencia de esos bugs tardan meses hasta proporcionar los parches de seguridad.

Los puntos sucesivos de este apartado incluyen una breve descripción de para que sirve la herramienta, la paquetería necesaria para su instalación, y sus ficheros de configuración más significativos. Y en los casos en los que aplique, una breve descripción de la interfaz WEB. Sin embargo, dado el número de ficheros de configuración manipulados y la extensión de los mismos, en lugar de añadir el contenido de éstos al correspondiente apartado de este capítulo, se proporcionaran en un DVD junto con la documentación del proyecto.

Por ultimo, antes de continuar, comentar que en el servidor de monitorización se ha instalado un sistema operativo Linux, en concreto, la distribución Centos 5.3, al que además se le ha añadido el repositorio rpmforge-release-0.5.1-1.el5.rf

7.4.1 Nagios

Nagios es un sistema de software libre para la gestión de equipos y servicios de red ampliamente utilizado, creado para ayudar a los administradores a controlar en cada momento qué está pasando en la red y conocer los problemas que ocurren en la infraestructura antes de que los usuarios de la misma los perciban. Proporciona gran versatilidad para consultar prácticamente cualquier parámetro de interés del sistema, y genera alertas que pueden ser recibidas por los responsables correspondientes, mediante correo electrónico y mensajes SMS, cuando los parámetros especificados exceden de los márgenes definidos por el administrador.

Entre sus características destacan la gestión de servicios de red y recursos de sistemas hardware (carga del procesador, uso de discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de gestionar la red de forma remota mediante túneles SSL cifrados ó SSH, el chequeo de servicios paralizados, la notificación de problemas y la posibilidad de programar plugins específicos para nuevos sistemas.

7.4.1.1 Paquetes a instalar

Toda la paquetería ha sido instalada vía yum install. Los paquetes necesarios son los siguientes:

- ✓ nagios-plugins-1.4.13-1.el5.rf
- ✓ nagios-plugins-nrpe-2.12-1.el5.rf
- ✓ nagios-3.2.0-1.el5.rf
- ✓ nagios-devel-3.2.0-1.el5.rf
- ✓ httpd-2.2.3-31.el5.centos.2 (Apache)

Y finalmente, con el fin de restringir la entrada a Nagios, mediante una contraseña de inicio:

1. Crear una lista de usuarios privilegiados contenida en el fichero htpasswd.users

   ```
   htpasswd -c /etc/nagios/htpasswd.users nagiosadmin
   ```

2. Editar el fichero /etc/httpd/conf.d/nagios.conf y añadir las directivas que le indiquen al servidor http donde encontrar la lista de usuarios y contraseñas creada en el paso 1.

   ```
   AuthUserFile /etc/nagios/htpasswd.users
   Require valid-user
   ```

7.4.1.2 Ficheros de configuración

Nagios divide en varios archivos las opciones de configuración, utilizando cada uno para definir diferentes parámetros para la gestión de la red. Así se encuentran dentro del directorio /etc/nagios/objects ocho ficheros de configuración.

Los tres primeros son utilizados en otros archivos de configuración, ya que definen los comandos, parámetros de tiempo y plantillas para los equipos y dispositivos. El cuarto fichero debe contener al menos un contacto válido, junto a su nombre y dirección de correo electrónico. Los cuatro últimos archivos se usan desde el fichero nagios.cfg y definen los equipos, dispositivos, topología de red, comandos, plantillas y contactos asociados.

Commands.cfg	Comandos de control instalados junto a Nagios. Algunos de ellos son el acceso por red de un equipo, su espacio en disco, la CPU usada, disponibilidad de servicios como hhtp, ftp, ssh, snmp o pop. Estos comandos son proporcionados a los equipos para definir los controles que se quieren asignar.
Templates.cfg	Colección de plantillas para ser utilizadas en contactos, equipos y servicios. Definen los periodos de tiempo, comandos de monitorizado o frecuencia de reintentos en casos de error, entre otros parámetros. Su uso permite aplicar un conjunto común de opciones a los elementos gestionados, haciendo más sencillo su cambio.
Timeperiods.cfg	Periodos de tiempo en que los comandos definidos en commands.cfg van a ejecutarse, y configuración de cuando se enviaran los mensajes de alerta a los contactos de contacts.cfg
Contacts.cfg	Contiene cada uno de los contactos con su nombre y dirección de correo electrónico. A cada elemento gestionado es necesario asignar al menos un contacto, al cual se le remitirá un mensaje en caso de generarse un estado de alerta.
Localhost.cfg	Controla los procesos y servicios del equipo en el que Nagios esta ejecutándose.
Printer.cfg	Control de impresoras.
Switch.cfg	Control de los switch.
Windows.cfg	Control de equipos y servicios de Windows.

Tabla 7-4 Nagios. Ficheros de configuración más significativos.

7.4.1.3 Interfaz WEB

Para acceder a la interfaz WEB de Nagios, abrir un navegador con la siguiente dirección e introducir usuario y contraseña.

http://localhost/nagios

Desde el menú principal, situado en la parte izquierda de la página, se acceden a las diferentes estadísticas generadas por Nagios, así como su estado actual. Los enlaces de mayor interés para el administrador son:

- Tactical overview (Ver Figura 7-7). Un completo resumen de todos los servicios y equipos en el momento actual, informando de las alertas críticas y advertencias, caídas, y de aquellos elementos que no tengan problemas. Su principal utilidad es ver en pocos segundos el estado completo de los elementos controlados.

- Service y Host Details (Ver Figura 7-8). Son los listados de servicios y equipos gestionados, respectivamente. Contienen su nombre, estado actual, fecha/hora de la última y próxima comprobación, y la salida del comando de monitorización.

- Service y Host Problem: Todos los servicios y equipos que presentan estado de error.

- Reporting: Un conjunto de opciones orientadas a generar informes con el historial de disponibilidad de equipos y servicios

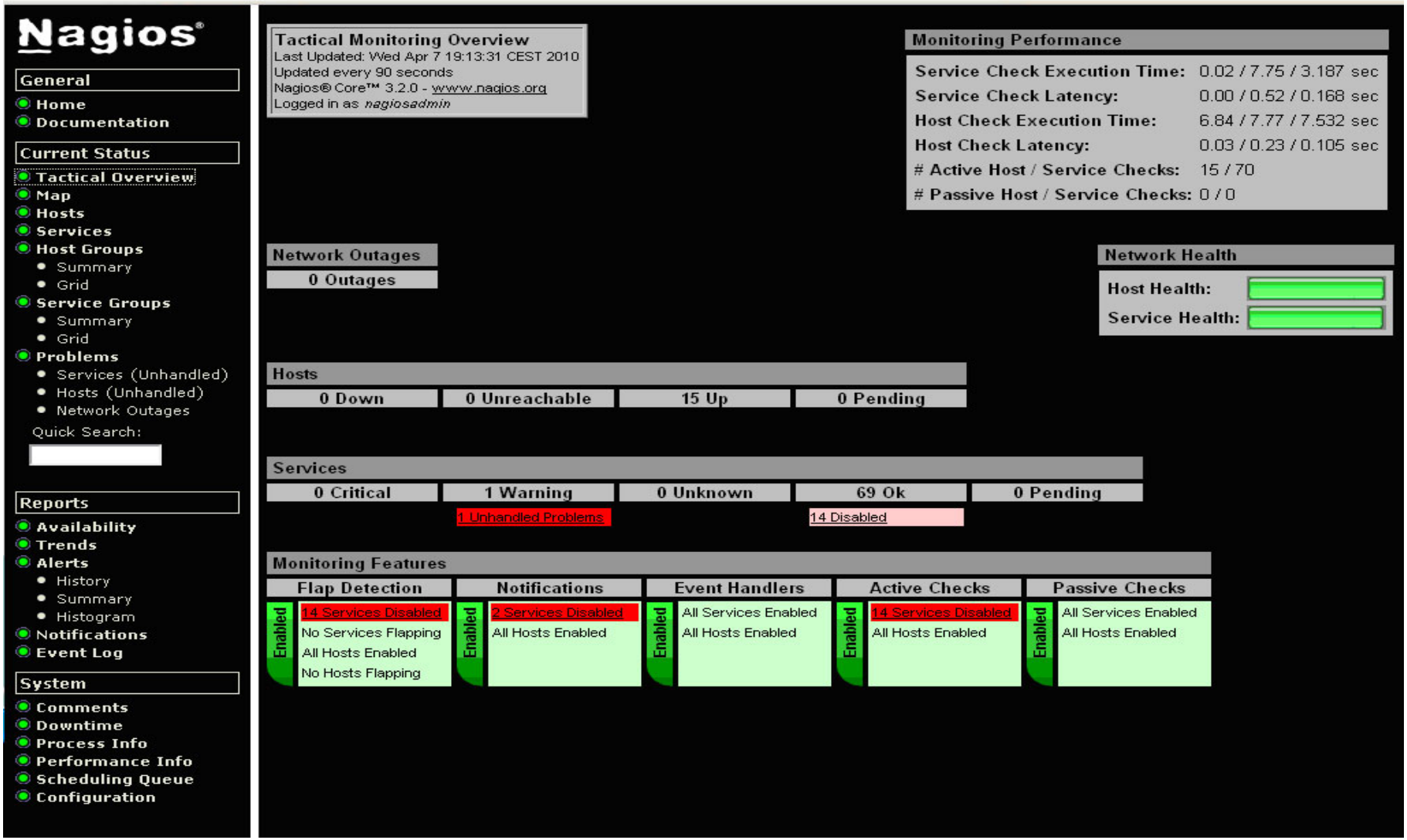


Figura 7-7 Nagios. Tactical Overview

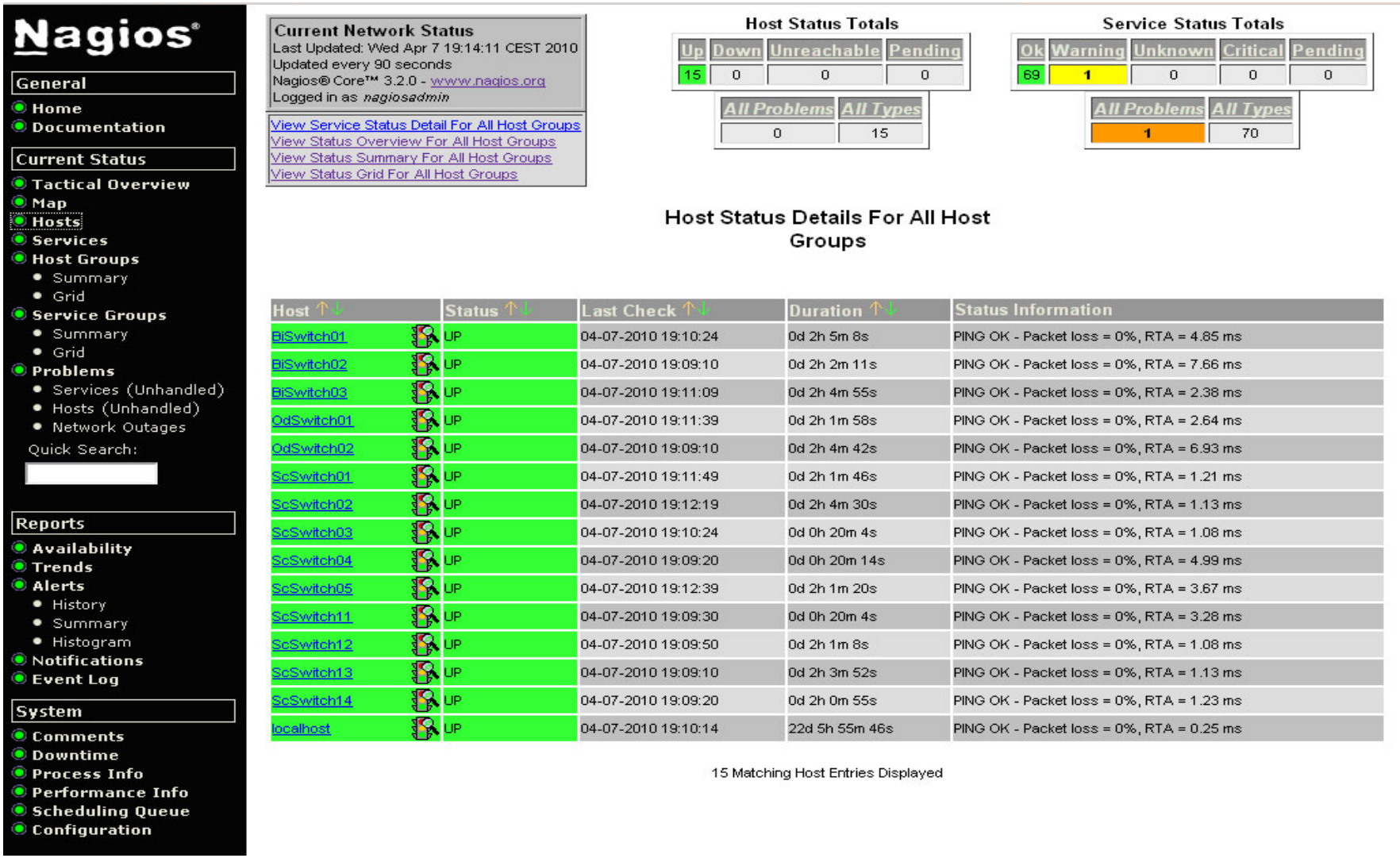


Figura 7-8 Nagios. Host Details

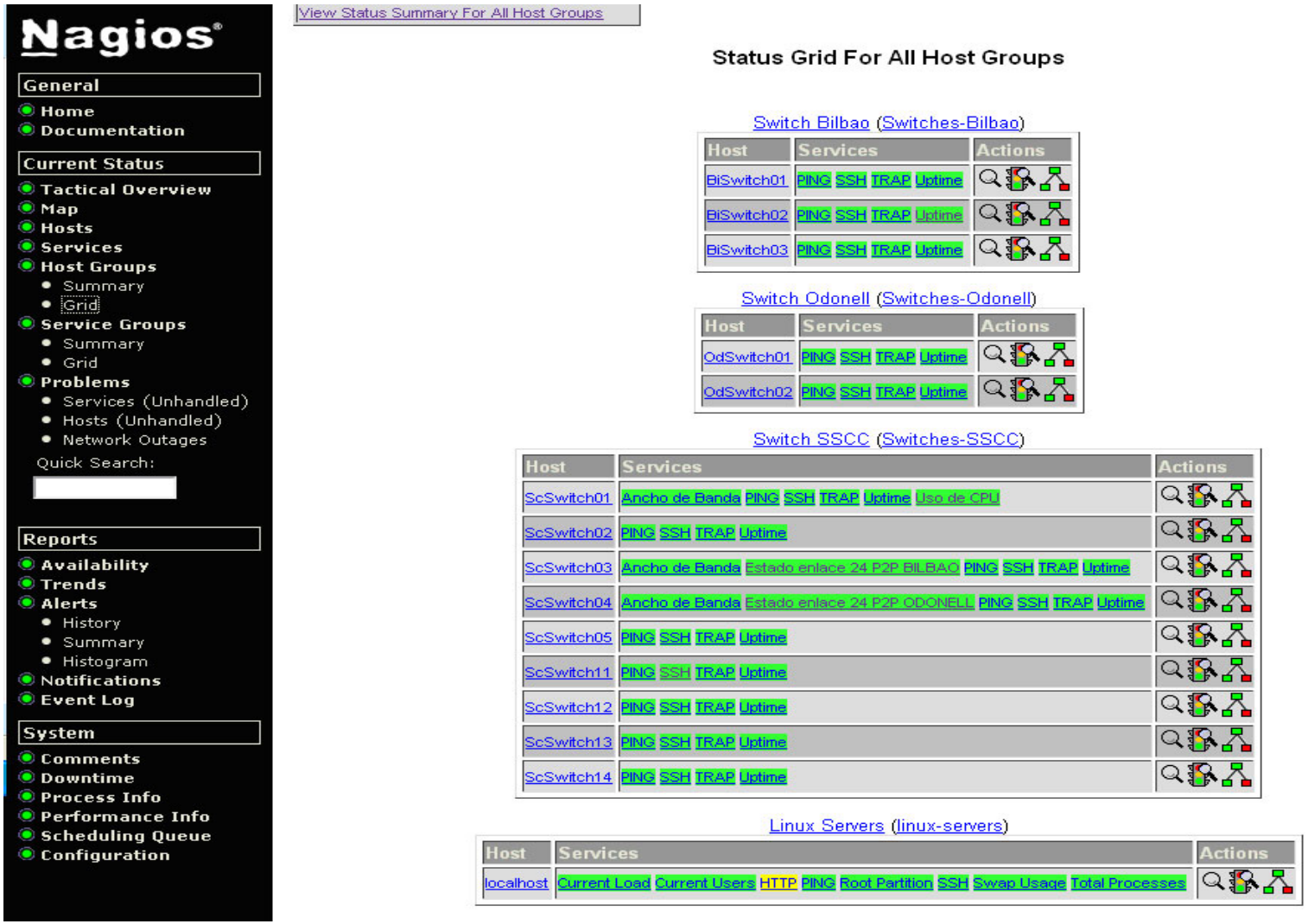


Figura 7-9 Resumen del Estado de todos los Servicios agrupado por Hosts y grupo

7.4.2 Cacti

Cacti es una completa solución de graficado en red, diseñada para aprovechar el poder de almacenamiento y la funcionalidad de graficar que poseen las RRDtool (Round Robin Data Base Tool), es decir, se trata de una herramienta que trabaja con una base de datos que maneja Planificación Round-Robin, según la cual la información se guarda siguiendo una trayectoria circular, sobrescribiendo los datos almacenados, una vez alcanzada la capacidad de la base de datos.

Cacti, desarrollada en PHP, provee un pooler ágil, plantillas de gráficos avanzadas, múltiples métodos para la recopilación de datos, y manejo de usuarios. Tiene una interfaz de usuario fácil de usar, que resulta conveniente para instalaciones del tamaño de una LAN, así como también para redes complejas con cientos de dispositivos.

7.4.2.1 Paquetes a instalar

Toda la paquetería ha sido instalada vía yum install. Los paquetes necesarios son los siguientes:

- ✓ cacti-0.8.7e-3.el5.rf
- ✓ php-mysql-5.1.6-24.el5_4.5
- ✓ perl-DBD-mysql-4.013-1.el5.rf
- ✓ mysql-5.0.77-4.el5_4.2
- ✓ mysql-server-5.0.77-4.el5_4.2

7.4.2.2 Interfaz WEB

Toda la configuración de Cacti se realiza vía Web. El objetivo que se busca con la herramienta es ver el ancho de banda consumido por cada usuario. A continuación se detalla cómo añadir un dispositivo a Cacti y como añadirle gráficos al dispositivo.

- **Paso 1**: Entrar en la Web de administración de Cacti e introducir usuario y contraseña.

  http://servidor/cacti/

Figura 7-10 Ventana de login de Cacti

- **Paso 2**: Antes de añadir los switches hay que cargar sus plantillas. Para ello es necesario descargar el fichero cacti_host_template_cisco_29003500.xml de la siguiente página:

  http://forums.cacti.net/about4843.html/

  A continuación, en la pestaña "console" acceder al menú de la izquierda y pinchar en la opción "Import Templates" para seleccionar el fichero descargado.

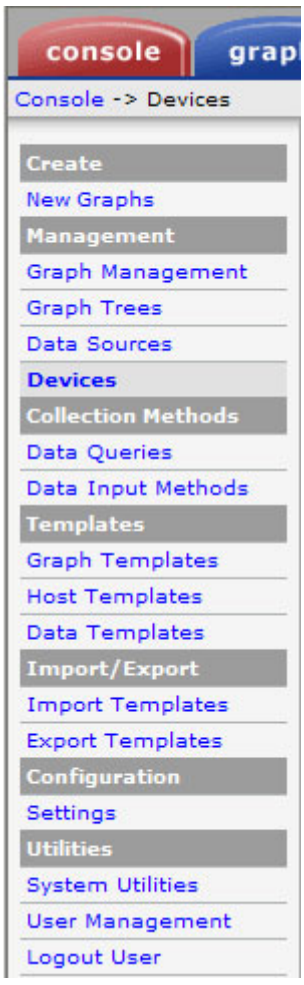


Figura 7-11 Menú Importar/Exportar plantillas

- **Paso 3:** Ahora ya se puede añadir un switch a Cacti desde la pestaña "console", pinchando en la opción "Device" (Ver Figura 7-11) y seguidamente haciendo clic arriba a la derecha en el botón "Add", como se ilustra en la siguiente figura.

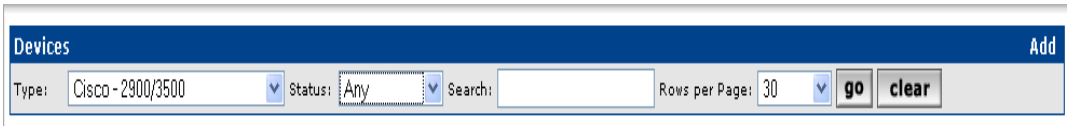


Figura 7-12 Opciones del menú Device

De este modo aparecerá un formulario donde hay que rellenar los datos del dispositivo que se desea añadir. En la Figura 7-13 se aprecia como los campos "Description" y "Hostname" se rellenan con el nombre del dispositivo, y en el campo hosts template se elije la plantilla, en este caso, Cisco–2900/3500. Por último, se especifican las opciones de SNMP, entre ellas la comunidad y la versión.

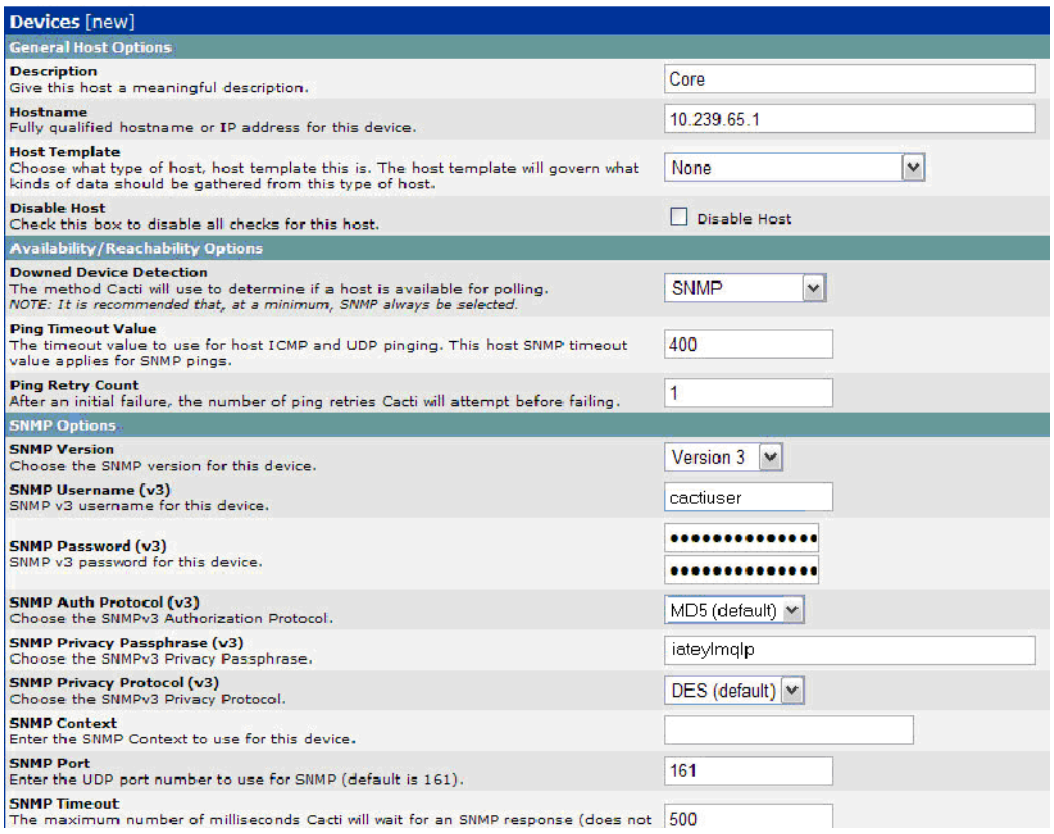


Figura 7-13 Opciones de configuración de un dispositivo

Tras finalizar el proceso, el dispositivo queda registrado.

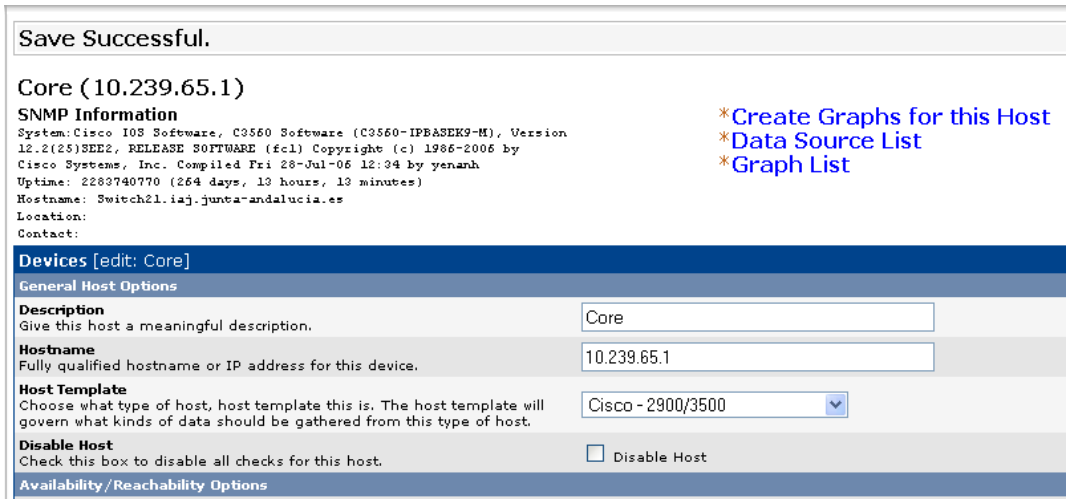


Figura 7-14 Dispositivo registrado con éxito

- **Paso 4:** El siguiente paso consiste en añadir el dispositivo creado al árbol de gráficos, ya que es el esquema organizativo dónde se encuentran todos los dispositivos que se están graficando. Para ver los árboles que se encuentran configurados, en la pestaña "console" (Ver Figura 7-11) pinchar en la opción "Graph Trees".

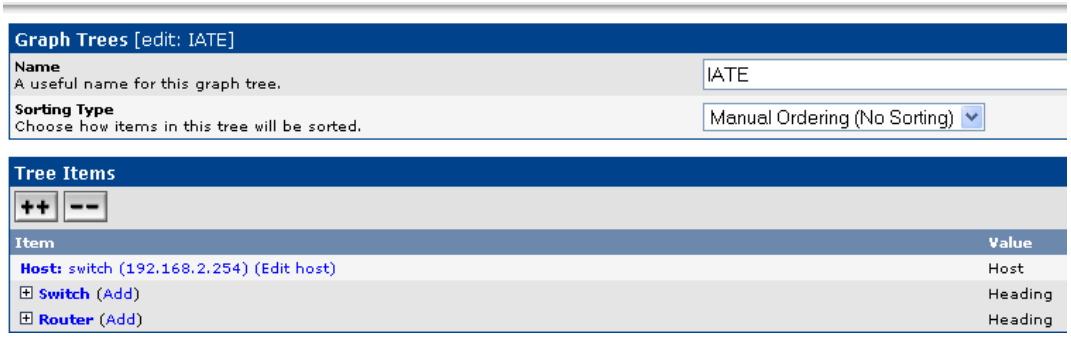


Figura 7-15 Menú Graph Trees.

Una vez aquí, elegir el árbol dónde se desea añadir el dispositivo. Al seleccionarlo aparecerá la lista de dispositivos que hay en ese árbol. Se pueden añadir tanto Hosts (dispositivos) como cabeceras, utilizadas para agrupar hosts y así organizar el árbol.

Pinchando en el botón "Add" aparecerá el formulario donde hay que rellenar los datos del elemento a añadir, indicando la cabecera desde la que colgará el elemento y si se trata de un host o de una cabecera. Si se elige host hay que especificar el nombre de host y si se trata de una cabecera el título de ésta.

- **Paso 5:** Sólo queda añadir gráficos al dispositivo. Para ello, desde la pestaña "console" (Ver Figura 7-11) acceder a la opción "New graphs". Aparecerá una nueva ventana en la cual hay que elegir el switch al que se le desean añadir gráficos. Una vez hecho esto,

aparecerán los elementos que se pueden graficar por SNMP, como por ejemplo el tráfico de las distintas interfaces. Se marcan los elementos que se quieren graficar, y tras pulsar la opción "Create" el resultado para el switch que se añadió en el paso 3 es el que muestra la siguiente figura.

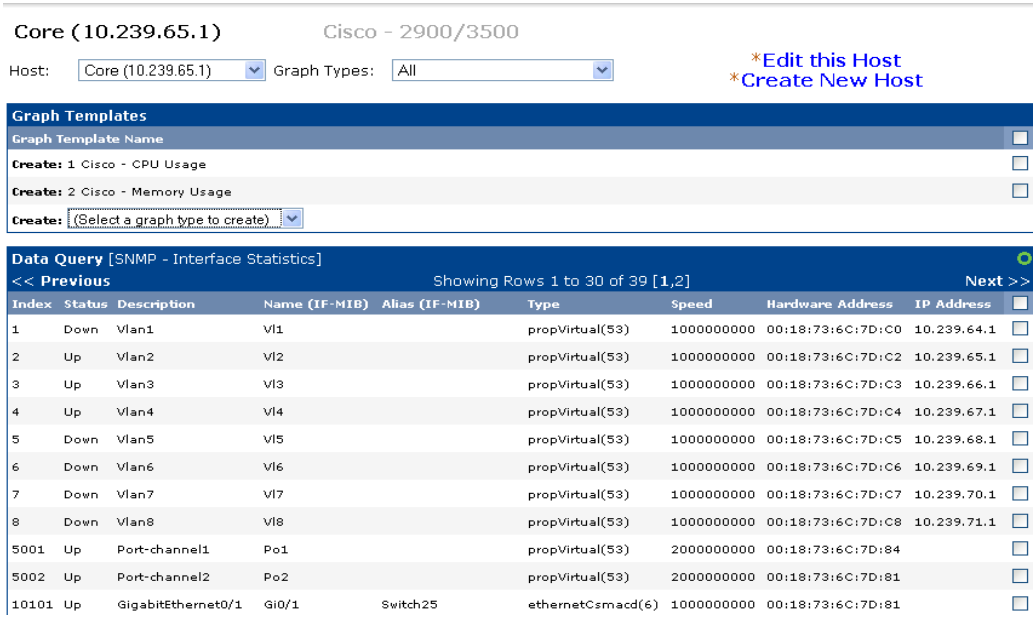


Figura 7-16 Datos obtenido por SNMP para el dispositivo 10.239.65.1

- **Paso 6:** Repetir los pasos 3,4 y 5 para cada uno de los switches.

Tras llevar a cabo correctamente todo el procedimiento, pasados unos minutos se comienzan a obtener resultados, a los cuales se pueden acceder desde la pestaña "Graphs" situada a la derecha de la pestaña "console".

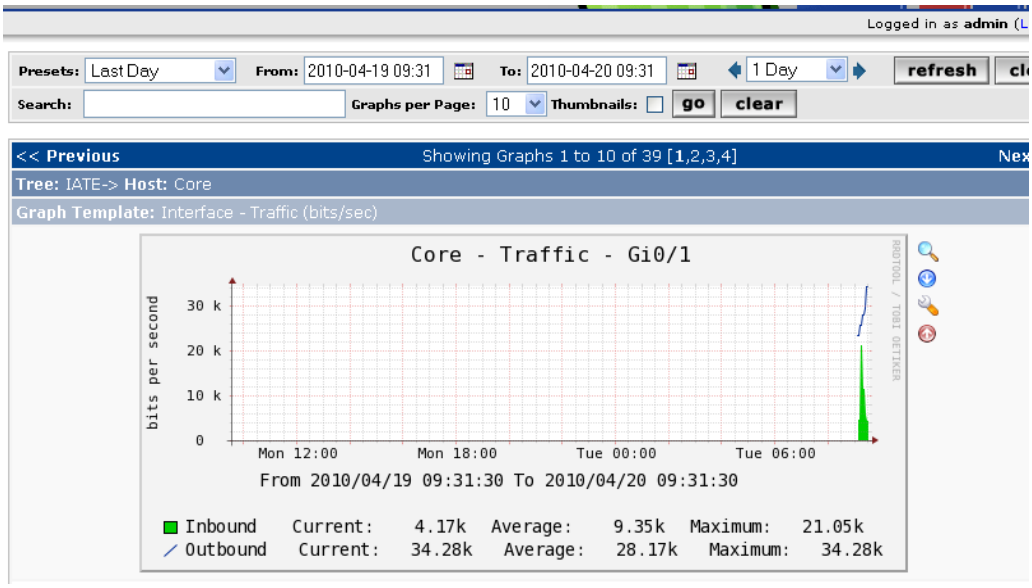


Figura 7-17 Representación gráfica de la Interfaz Gigabits 0/1

Por otra parte, comentar que la nomenclatura para dar nombre a los gráficos con los que se trabaja en el IATE sigue la siguiente regla: Nombre del switch – Traffic – Interfaz – Equipo. Con este formato se clasifica de forma univoca el tráfico que pasa por el switch. De este modo, la Figura 7-18 se aprecia claramente que corresponde al Host SSCC059, que está en la boca Fa0/1 del switch 11.

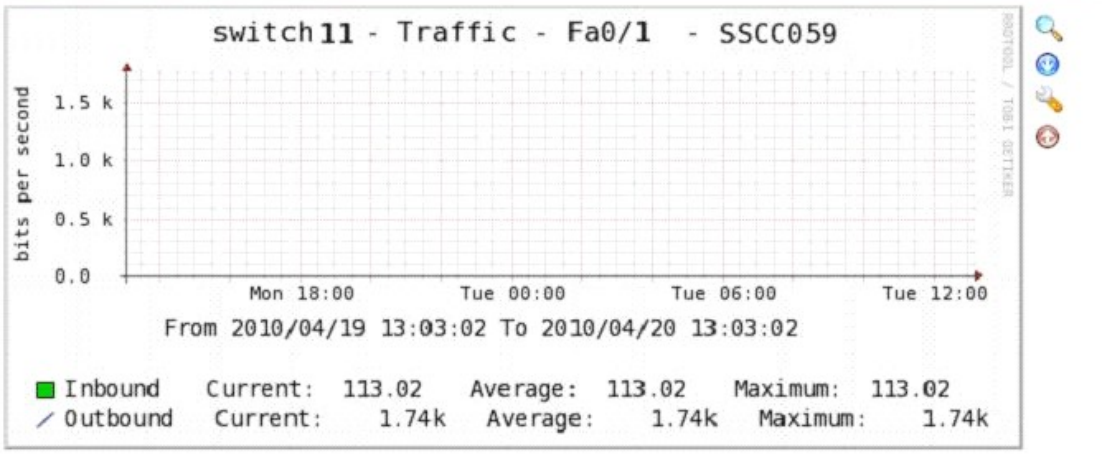


Figura 7-18 Gráfica del ancho de banda para el equipo SSCC059

7.4.3 Subversión

Subversión es un software para el control de versiones, que administra el acceso a un conjunto de ficheros y mantiene un historial de cambios realizados. Normalmente consiste en una copia maestra almacenada en un repositorio central, y un programa cliente con el que cada usuario sincroniza su copia local. Esto permite compartir los cambios sobre un mismo conjunto de ficheros, guardar registro de los cambios realizados por cada usuario, y volver a un estado anterior en caso de necesidad.

Con la implantación de subversión se ha facilitado el control y mantenimiento de la documentación de red, cuya responsabilidad recae en el administrador de la red. La documentación de red es imprescindible para facilitar la gestión de la red.

7.4.3.1 Paquetes a instalar

Toda la paquetería ha sido instalada vía yum install. Los paquetes necesarios son los siguientes:

- ✓ subversion i386 1.4.2-2.el5 base 2.3 M
- ✓ perl-URI noarch 1.35-3 base 116 k
- ✓ mod_dav_svn i386 1.4.2-2.el5 base 70 k

7.4.3.2 Ficheros de configuración

subversion.conf	Situado en /etc/httpd/conf.d/. En este fichero se va especificar: ▪ Ruta donde estará situado el repositorio, con la directiva SVNPath. ▪ Ruta donde estará situado el fichero de autenticación con AuthUserFile /etc/svn-auth-conf ▪ Ruta donde encontrar las listas de control de acceso (ACL) al repositorio. AuthzSVNAccessFile /etc/svn-acl-conf
svn-auth-conf	Situado en /etc/svn-auth-conf define los usuarios y contraseñas. Inicialmente se utiliza el comando htpasswd con argumento –cm. De este modo se crea un fichero con contraseñas encriptadas mediante MD5 (Message-Digest Algorithm 5 o Algoritmo de Resumen del Mensaje). htpasswd -cm /etc/svn-auth-conf yourusername Si necesita adicionar más usuarios, después de la creación inicial, se utilizará solo el argumento -m Htpasswd -m /etc/svn-auth-conf yourusername
svn-acl-conf	Situado en /etc/svn-acl-conf sirve para definir las ACL. Este fichero está formado por secciones de la forma siguiente: [reponame:repopath] user = access Donde access puede ser r (lectura), rw (lectura y escritura), o vacío para ningún acceso. La ACL por defecto niega el acceso de los usuarios al repositorio.

Tabla 7-5 Subversión. Fichero de configuración.

Una vez se ha configurado el fichero subversion.conf de acuerdo a las necesidades del IATE, quedan dos pasos para completar el proceso:

- Crear el repositorio
- Restringir el acceso a los repositorios.

Para crear el repositorio se aplican los siguientes comandos Linux.

```
cd /var/www/
mkdir svn
cd svn
```

```
svnadmin create repos
chown -R apache.apache repos
service httpd restart
```

Una vez creado el repositorio, ya que habitualmente no es necesario que todos los usuarios tengan acceso a todos los repositorios, se restringe el acceso por usuario, mediante el uso de ACLs (Access Control Lists o Listas de Control de Acceso).

```
vim /etc/svn-acl-conf
Se añade [repos:/]
        admin = rw
        tecnicos = r
```

7.4.3.3 Cliente subversión

El cliente elegido para trabajar con Subversión ha sido TortoiseSVN, por ser ampliamente utilizado en el mercado. Esta aplicación se puede descargar de:

http://tortoisesvn.tigris.org/

Una vez instalado, la herramienta TortoiseSVN se integra dentro del explorador de Windows. Para utilizarla solo es necesario abrir el explorador de Windows y hacer clic con el botón derecho del ratón en cualquier carpeta donde se desee ejecutar algún comando del TortoiseSVN.

La instalación del cliente es sencilla y no requiere configuración personalizada de la herramienta. Sin embargo, como se verá a continuación, es necesario realizar algunos pasos extras para obtener una copia del repositorio en la maquina cliente y poder acceder a los ficheros del repositorio.

1. Crear una carpeta en el directorio de trabajo, en nuestro caso “Documentacion de red”. Situarse encima de dicha carpeta y con el botón derecho del ratón acceder a la opción “SVN Obtener”, para descargar una copia del repositorio en la carpeta creada. La Figura 7-19 ilustra la ventana que se muestra al pulsar dicha opción. En ella hay que indicar la dirección de la cual obtener el repositorio y la ruta al directorio “Documentación de red”.

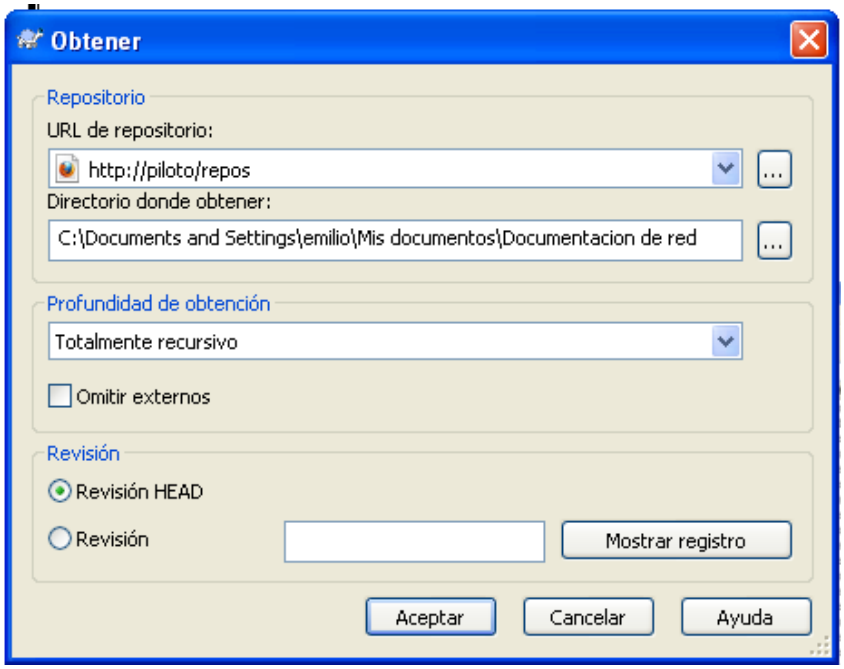


Figura 7-19 Cliente Subversión. Opción SNV Obtener

Una vez pulsado el botón Aceptar, solicita nombre de usuario y contraseña. Tras autenticarse, el repositorio se descarga en la maquina local y la carpeta "Documentacion de red" adquiere el siguiente aspecto.

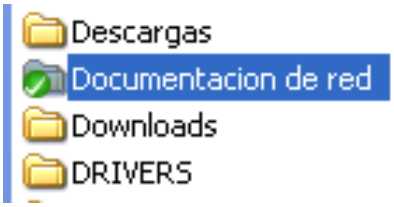


Figura 7-20 Cliente Subversión. Repositorio descargado

2. Si en su equipo local el administrador realiza cambios en la documentación de la red, es necesario enviarlos al repositorio almacenado en el servidor. Este proceso se conoce como confirmar los cambios.

   Antes de confirmar hay que asegurarse de que la copia de trabajo está actualizada con respecto al servidor. Para ello se puede utilizar la opción "SVN Actualizar" o bien ejecutar "TortoiseSVN → Comprobar modificaciones". De este modo se comprueba si los cambios se han originado localmente o en el servidor. Finalmente, si todo es correcto se confirman los cambios mediante la opción "SVN Confirmar" y el repositorio almacenado en el servidor recogerá las modificaciones que se hayan hecho en el equipo cliente.

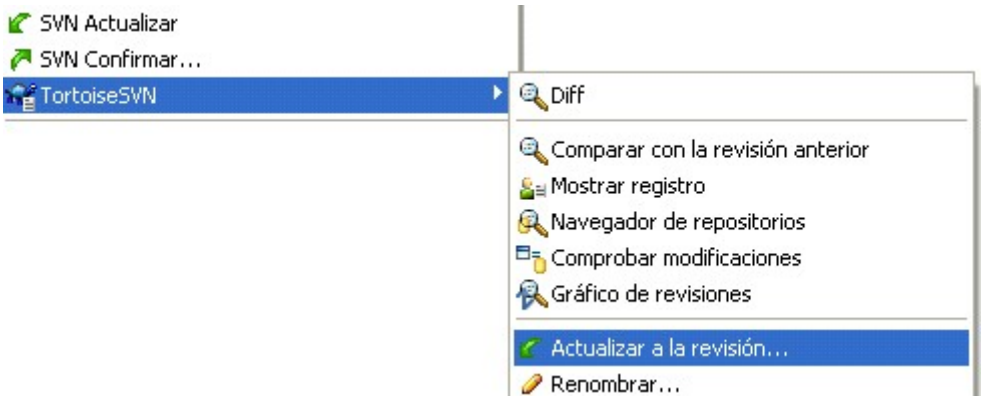


Figura 7-21 Cliente Subversión. Actualizar/Confirmar repositorio

La herramienta subversión dispone de otras opciones, tales como recuperar versiones anteriores, editor para resolver conflictos entre ficheros, etc...., que permiten trabajar de manera sencilla con el subversión instalado.

7.5 Implantación de la gestión de red en el IATE

Una vez definida la arquitectura lógica para el sistema de gestión de la red, tras establecer los puntos críticos susceptibles de ser controlados y elegir las herramientas a utilizar para las actividades de control, solo queda definir un conjunto de parámetros significativos para gestionar la red del IATE.

- Disponibilidad de los servicios de los dispositivos
- Control de la CPU del switch de capa 3
- Control del ancho de banda

ScSwitch01	Ancho de Banda	OK	04-07-2010 19:10:07	0d 0h 14m 14s	1/3	OK Out: 179.59Kbps: In: 423.65Kbps
	PING	OK	04-07-2010 19:12:27	0d 2h 1m 56s	1/3	PING OK - Packet loss = 0%, RTA = 27.21 ms
	SSH	OK	04-07-2010 19:14:03	0d 0h 5m 18s	1/3	SSH OK - Cisco-1.25 (protocol 1.99)
	TRAP PASV	OK	04-07-2010 19:13:58	0d 0h 18m 31s	1/1	PING OK - Packet loss = 0%, RTA = 1.06 ms
	Uptime	OK	04-07-2010 19:07:24	0d 1h 46m 57s	1/3	SNMP OK - Timeticks: (2175119891) 251 days, 17:59:58.91
	Uso de CPU	OK	04-07-2010 19:05:38	0d 1h 31m 19s	1/3	CPU usage 1min/5min OK - 4 / 4

Figura 7-22 Resumen de parámetros a gestionar en el IATE

7.5.1 Disponibilidad de los servicios de los dispositivos.

Los chequeos asociados a la disponibilidad de los dispositivos, que se van a detallar a continuación son:

- PING. Con este chequeo se comprueba que el dispositivo esta levantado
- SSH. Con este chequeo se comprueba que es posible el acceso al dispositivo
- UPTIME. Con este chequeo se comprueba el tiempo que el dispositivo se encuentra levantado.

La herramienta empleada para llevar a cabo esta tarea ha sido el Nagios. Uno de los chequeos programados consiste en el envío de un ping a los dispositivos monitorizados para ver si están levantados. Si Nagios detecta que el dispositivo está caído, alertará al administrador mediante un correo.

En la Figura 7-23 se puede ver el estado de los servicios agrupados por Host. Como se aprecia en ella, el servicio de ping (PING) es utilizado por todos los elementos a controlar. Toda la electrónica de red y los puentes inalámbricos tienen que estar levantado las 24 horas del día. Nagios controla esta situación mostrando un "OK" en el servicio de ping y un indicador de color verde.

Cuando Nagios detecta que un dispositivo se ha caído, el mensaje mostrado es "CRITICAL", resaltado mediante el color rojo, como ilustra la Figura 7-23 en el scSwitch11. En tal caso, Nagios además alerta al administrador a través de un correo con el siguiente contenido:

"***** Nagios *****
Notification Type: PROBLEM
Host: ScSwitch11
State: DOWN
Address: 10.239.71.11
Info: CRITICAL - Host Unreachable (10.239.71.11)
Date/Time: Sun Apr 7 19:14:15 CEST 2010"

El acceso de los dispositivos se realiza por ssh, el Telnet va a quedar deshabilitado. Nagios permite monitorizar el servicio SSH. Si todo está correcto mostrará un "OK" mientras que si se detecta algún problema mostrará un mensaje tipo "CRITICAL", como refleja la Figura 7-23 en el ScSwitch04 y el siguiente email.

"***** Nagios *****
Notification Type: PROBLEM
Service: SSH
Host: ScSwitch04
Address: 10.239.72.4
State: CRITICAL
Date/Time: Sun Apr 7 19:14:20 CEST 2010
Additional Info: Conexión rehusada"

Otro de los chequeos, conocidos como Uptime, muestra el tiempo que el dispositivo lleva levantado, y esto ayuda a detectar un “falso positivo”, una alerta generada por la caída de un dispositivo que realmente no lo está.

	BILBAO	OK				
	PING	OK	04-07-2010 19:13:49	0d 0h 20m 32s	1/3	PING OK - Packet loss = 0%, RTA = 1.90 ms
	SSH	OK	04-07-2010 19:13:04	0d 0h 1m 17s	1/3	SSH OK - Cisco-1.25 (protocol 1.99)
	TRAP	OK	04-07-2010 19:13:58	0d 0h 18m 31s	1/1	PING OK - Packet loss = 0%, RTA = 14.50 ms
	Uptime	OK	04-07-2010 19:05:09	0d 1h 49m 12s	1/3	SNMP OK - Timeticks: (924096202) 106 days, 22:56:02.02
ScSwitch04	Ancho de Banda	OK	04-07-2010 19:10:18	0d 0h 14m 3s	1/3	OK Out: 33.18Kbps: In: 266.31Kbps
	Estado enlace 24 P2P ODONELL	OK	04-07-2010 19:08:26	0d 0h 26m 1s	1/3	SNMP OK - up(1)
	PING	OK	04-07-2010 19:12:11	0d 2h 4m 27s	1/3	PING OK - Packet loss = 0%, RTA = 1.87 ms
	SSH	CRITICAL	04-07-2010 19:14:12	0d 0h 5m 9s	1/3	CRITICAL - Socket timeout after 10 seconds
	TRAP	OK	04-07-2010 19:13:58	0d 0h 18m 31s	1/1	PING OK - Packet loss = 0%, RTA = 13.93 ms
	Uptime	OK	04-07-2010 19:04:59	0d 0h 19m 22s	1/3	SNMP OK - Timeticks: (141443402) 16 days, 8:53:54.02
ScSwitch05	PING	OK	04-07-2010 19:10:19	0d 2h 1m 30s	1/3	PING OK - Packet loss = 0%, RTA = 3.79 ms
	SSH	OK	04-07-2010 19:11:12	0d 0h 3m 9s	1/3	SSH OK - Cisco-1.25 (protocol 1.99)
	TRAP	OK	04-07-2010 19:13:58	0d 0h 18m 31s	1/1	PING OK - Packet loss = 0%, RTA = 7.98 ms
	Uptime	OK	04-07-2010 19:07:46	0d 1h 49m 2s	1/3	SNMP OK - Timeticks: (141460095) 16 days, 8:56:40.95
ScSwitch11	PING	CRITICAL	04-07-2010 19:14:06	0d 0h 54m 7s	1/3	CRITICAL - Host Unreachable
	SSH	CRITICAL	04-07-2010 19:14:02	0d 0h 4m 7s	1/3	CRITICAL - Socket timeout after 10 seconds
	TRAP	CRITICAL	04-07-2010 19:13:58	0d 1h 0m 59s	1/1	CRITICAL - Host Unreachable
	Uptime	UNKNOWN	04-07-2010 19:07:44	0d 0h 54m 7s	1/3	SNMP problem - No data received from host
ScSwitch12	PING	OK	04-07-2010 19:10:32	0d 2h 1m 18s	1/3	PING OK - Packet loss = 0%, RTA = 1.12 ms
	SSH	OK	04-07-2010 19:12:20	0d 0h 7m 1s	1/3	SSH OK - Cisco-1.25 (protocol 1.99)
	TRAP	OK	04-07-2010 19:13:58	0d 0h 18m 31s	1/1	PING OK - Packet loss = 0%, RTA = 2.80 ms
	Uptime	OK	04-07-2010 19:05:48	0d 1h 51m 17s	1/3	SNMP OK - Timeticks: (2175495718) 251 days, 19:02:37.18
ScSwitch13	PING	OK	04-07-2010 19:10:11	0d 2h 4m 2s	1/3	PING OK - Packet loss = 0%, RTA = 1.51 ms
	SSH	OK	04-07-2010 19:09:20	0d 0h 5m 1s	1/3	SSH OK - Cisco-1.25 (protocol 1.99)
	TRAP	OK	04-07-2010 19:13:58	0d 0h 18m 31s	1/1	PING OK - Packet loss = 0%, RTA = 1.46 ms
	Uptime	OK	04-07-2010 19:05:29	0d 1h 48m 52s	1/3	SNMP OK - Timeticks: (129957522) 15 days, 0:59:35.22
ScSwitch14	PING	OK	04-07-2010 19:09:16	0d 0h 20m 5s	1/3	PING OK - Packet loss = 0%, RTA = 2.34 ms
	SSH	OK	04-07-2010 19:11:21	0d 0h 3m 0s	1/3	SSH OK - Cisco-1.25 (protocol 1.99)
	TRAP	OK	04-07-2010 19:13:58	0d 0h 18m 31s	1/1	PING OK - Packet loss = 0%, RTA = 1.34 ms
	Uptime	OK	04-07-2010 19:07:55	0d 1h 46m 26s	1/3	SNMP OK - Timeticks: (2175122579) 251 days, 18:00:25.79

Figura 7-23 Estado de los Servicio agrupados por Host

7.5.2 Control de la CPU del switch de capa 3

Para ver si la CPU del switch principal del IATE soporta correctamente todo el tráfico generado en el IATE, se ha utilizado una vez más Nagios.

cSwitch01	Ancho de Banda	OK	04-07-2010 19:10:07	0d 0h 14m 14s	1/3	OK Out: 179.59Kbps: In: 423.65Kbps
	PING	OK	04-07-2010 19:12:27	0d 2h 1m 56s	1/3	PING OK - Packet loss = 0%, RTA = 27.21 ms
	SSH	OK	04-07-2010 19:14:03	0d 0h 5m 18s	1/3	SSH OK - Cisco-1.25 (protocol 1.99)
	TRAP PASV	OK	04-07-2010 19:13:58	0d 0h 18m 31s	1/1	PING OK - Packet loss = 0%, RTA = 1.06 ms
	Uptime	OK	04-07-2010 19:07:24	0d 1h 46m 57s	1/3	SNMP OK - Timeticks: (2175119891) 251 days, 17:59:58.91
	Uso de CPU	OK	04-07-2010 19:05:38	0d 1h 31m 19s	1/3	CPU usage 1min/5min OK - 4 / 4

Figura 7-24 Uso de CPU del switch principal del IATE

Como se observa en la figura, se realiza un chequeo de la CPU por SNMP. Si el estado del indicador "Uso de CPU" es distinto de "OK", el administrador investigaría las causas que están provocando la carga de CPU (posible ataque, que el switch no pudiera conmutar todo el trafico que le llega, etc…)

7.5.3 Control del ancho de banda.

En esta ocasión, las herramientas empleadas han sido Nagios, Cacti. Ntop también es útil para controlar el ancho de banda utilizado en la red, como se vio en el capitulo 4.

En Nagios el chequeo del ancho de Banda controla que los usuarios no dejen congestionada la salida a Internet, ni que se produzcan cuellos de botella en los enlaces P2P (Peer to peer o punto a punto) entre los puentes inalámbricos.

Si el consumo de ancho de banda de Internet es inferior al 75%, Nagios muestra un "OK", como refleja la Figura 7-24 en el scSwitch01. Si es superior al 75% del ancho de banda alertará con un "WARNING", y si supera el 90% aparecerá un "CRITICAL".

En los enlaces punto a punto mostrará un "WARNING" si supera el 10% del ancho de banda, y si supera el 20% aparecerá un "CRITICAL", ya que hay que tener en cuenta que de los 54 Mbps, la transmisión queda alrededor de 25 Mbps.

La Figura 7-25 indica que el ancho de banda en el Switch que conecta con el puente inalámbrico que apunta a Bilbao se encuentra congestionado, así que el administrador es alertado con un correo.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
ScSwitch06	Ancho de Banda Boca 24	CRITICAL	05-02-2010 11:30:18	0d 0h 1m 19s	3/3	CRITICAL Out: 588.53Kbps: In: 23.72Mbps
	Estado enlace 24 P2P BILBAO	OK	05-02-2010 11:21:08	0d 1h 19m 16s	1/3	SNMP OK - up(1)
	PING	OK	05-02-2010 11:25:55	0d 0h 19m 28s	1/3	PING OK - Packet loss = 0%, RTA = 1.25 ms
	SSH	OK	05-02-2010 11:21:08	0d 0h 59m 20s	1/3	SSH OK - Cisco-1.25 (protocol 1.99)
	TRAP	OK	05-02-2010 11:27:52	0d 1h 17m 21s	1/1	PING OK - Packet loss = 0%, RTA = 1.88 ms
	Uptime	OK	05-02-2010 11:24:23	0d 1h 16m 0s	1/3	SNMP OK - Timeticks: (593241) 1:38:52.41

Figura 7-25 Ancho de Banda en el enlace punto a punto con Bilbao

"***** Nagios *****

Notification Type: PROBLEM

Service: Ancho de Banda Boca 24 BILBAO

Host: ScSwitch06

Address: 10.239.72.6

State: CRITICAL

Date/Time: Sun May 2 11:30:20 CEST 2010

Additional Info: CRITICAL Out: 588.53Kbps: In: 23.7Mbps"

Por otra parte, Cacti controla el ancho de banda consumido por cada switch. Parámetros de especial interés son el ancho de banda consumido en el acceso a Internet, puntos de acceso inalámbrico, y conexión con los switch de servidores. A continuación se muestra una captura del ancho de banda consumido por el switch06 y su enlace 24, que une Muñoz Olivé con Bilbao.

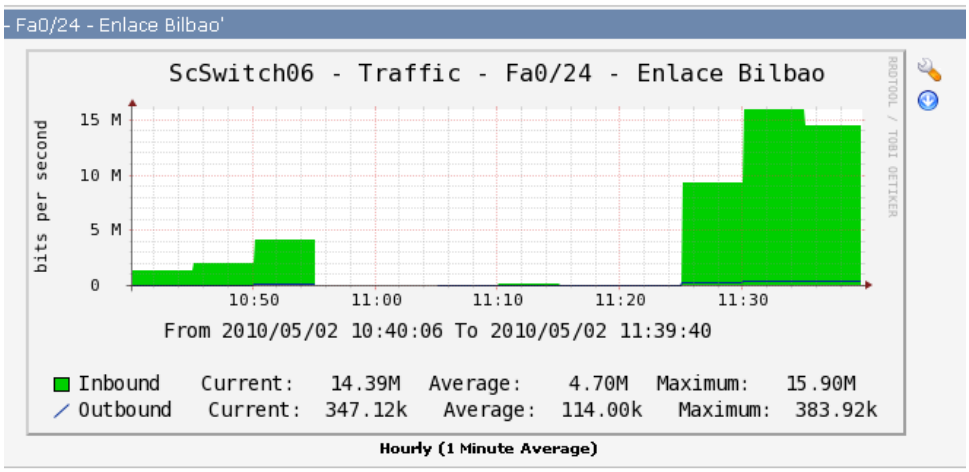


Figura 7-26 Ancho de Banda consumido por el Switch que une con Bilbao

Esta figura muestra como el ancho de banda consumido desde 10:50 a 11:25 no presenta problemas, ya que el tráfico en este tramo es prácticamente nulo, mientras que luego se refleja un consumo del ancho de banda, provocando una saturación del canal. Para ver que usuarios están congestionando el canal a partir de las 11.30, una práctica habitual es complementar esta información con los datos obtenidos mediante el Ntop, como ya se trató en el capitulo 4.

7.6 Conclusiones

Los objetivos de una infraestructura de gestión de la red de sistemas informáticos son principalmente la prevención de incidencias, conocer el aprovechamiento de los recursos disponibles, y alertar ante cualquier problema que pueda provocar la pérdida del servicio. Dado que estos objetivos son importantes en cualquier entidad independientemente de su tamaño, es evidente que toda organización debería contar con su propio sistema de gestión de la red.

A lo largo del capitulo las actividades de gestión de red se han enfocado en tres puntos fundamentales: controlar la disponibilidad de los dispositivos mediante la revisión de su estado a través de logs, controlar la CPU del switch más poderoso, y tratar de evitar la saturación del ancho de banda. Complementado todo ello con una buena gestión de la documentación de red.

Aunque parezca lo contrario, implementar un buen sistema de gestión de la red no es una tarea tan difícil como exigente en su ejecución. Como se ha visto en este capítulo, el primer paso consiste en realizar un análisis detallado del sistema informático a controlar para, entre otras cosas, detectar los sistemas críticos (tanto máquinas como servicios) y formular políticas de actuación frente a incidencias en dichos sistemas.

El siguiente paso es seleccionar el paquete software para la gestión de la red. Afortunadamente, hoy día existe un amplio abanico de herramientas de licencia libre, las cuales destacan especialmente por su flexibilidad para poder monitorizar todo lo que se desee. Entre ellas se encuentran Nagios, Syslog y Cacti. Por su parte, para el control de configuración de la documentación de red se ha optado por Subversion.

Tras la instalación y configuración de las mismas, en el último apartado del capítulo, se han recogido los resultados de controlar en el IATE parámetros como la disponibilidad de los servicios de los dispositivos, la CPU del switch de capa 3 y el ancho de banda consumido. Los ejemplos aquí expuestos demuestran que el uso de estas herramientas permite controlar el estado de los elementos controlados de forma fácil y ágil, garantizando el buen mantenimiento de la red a través de alertas al administrador que le permiten actuar de inmediato en la resolución de cualquier incidencia.

Capítulo 8.

Plan de pruebas

8.1 Introducción

En este capítulo se recoge el plan de pruebas elaborado para demostrar que se han alcanzado los objetivos propuestos y que se cumple con los requisitos expuestos en capítulos anteriores.

Las pruebas aquí descritas se han realizado en los equipos de la red del IATE con el fin de conseguir la certificación que acredita que se han cumplido los requisitos exigidos por el cliente. Sin embargo, por políticas de privacidad de la empresa resulta imposible mostrar fotografías del entorno real, y en su defecto, al final del capítulo se muestran imágenes del pequeño laboratorio, utilizado en las primeras fases del proyecto para simular la red. En ambos entornos, el resultado obtenido es el esperado.

8.2 Listado de Pruebas

Las distintas pruebas que se han llevado a cabo durante la fase de certificación se encuentran recogidas en la tabla que se muestra a continuación.

Código	Descripción
PR-01	Conectividad
PR-02	Enrutado entre VLANs
PR-03	Comprobación del puente raíz
PR-04	Aislamiento entre VLANs
PR-05	Seguridad en el acceso a los switches
PR-06	Alta disponibilidad en capa 2
PR-07	Alta disponibilidad en capa 3 e Interfaz de tracking
PR-08	Asignación de IP por DHCP

Tabla 8- 1 Listado de pruebas

En los apartados sucesivos se exponen y explican las pruebas aquí enumeradas, y luego se comentan los resultados.

En este capitulo no se documentan las pruebas que demuestran que las medidas de seguridad implementadas combaten los ataques más comunes de capa 2, puesto que ya fueron descritas anteriormente en el capítulo de seguridad.

8.3 Prueba PR-01: Conectividad

Esta prueba consiste en verificar que hay respuesta de todos los dispositivos de la red. Para ello, se lanza un ping a los switches de la capa núcleo, ScSwitch01 y ScSwitch02. Una vez que éstos responden, se realiza la misma prueba al resto de dispositivos de red. Las siguientes figuras muestran que el resultado es satisfactorio, quedando patente que existe conectividad entre todos los equipos.

Como se observa en la figura, en primer lugar se hace ping a la interfaz HSRP de la VLAN 2 de informática.

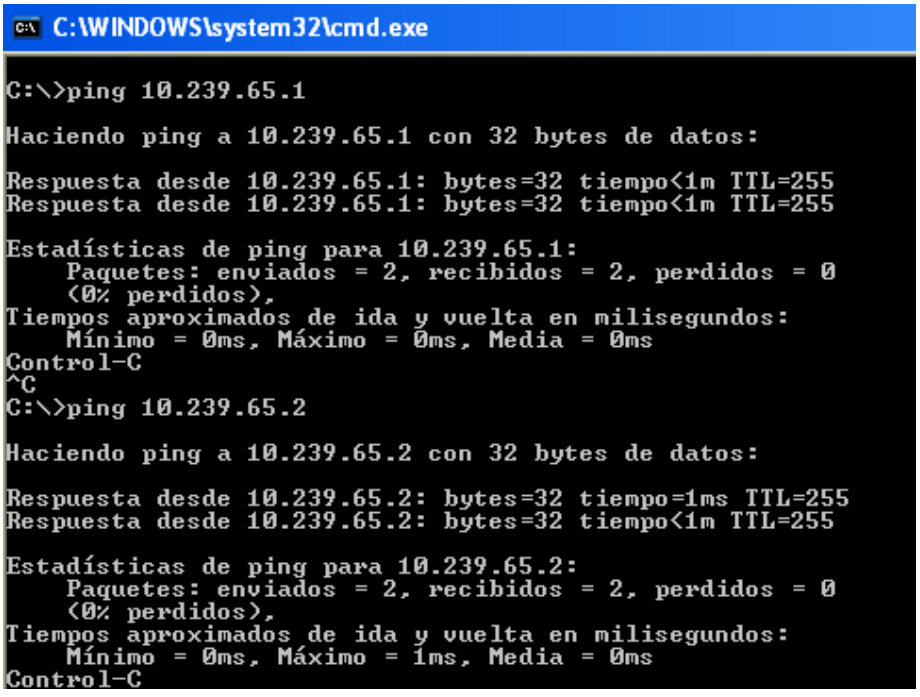


Figura 8-1 Conectividad con IP HSRP

A continuación se lanza ping a la interfaz de la VLAN 2 del switch ScSwitch01 y a la interfaz de la VLAN 2 del switch ScSwitch02.

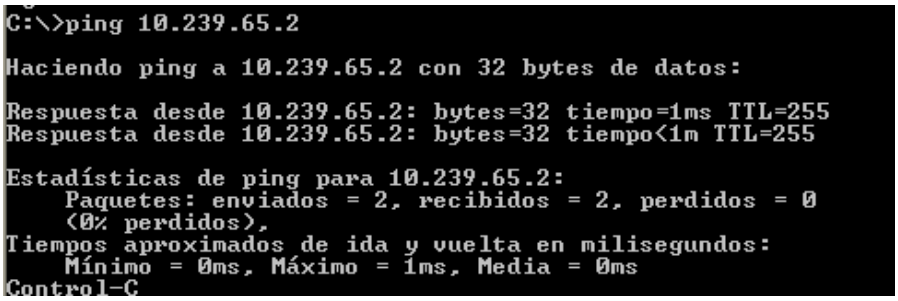


Figura 8-2 Conectividad con VLAN de informática ScSwitch01

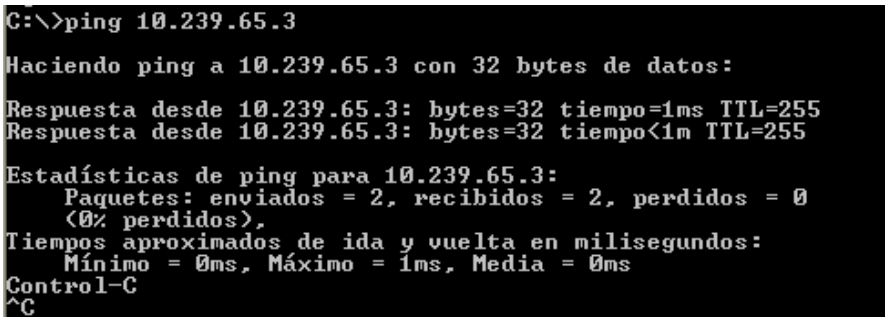


Figura 8-3 Conectividad con VLAN de informática ScSwitch02

Seguidamente, se realiza la misma prueba para la VLAN de servidores.

Figura 8-4 Conectividad con VLAN de servidores

Se repite la misma prueba para cada uno de los dispositivos de red y en todos los casos el resultado obtenido es analógo al presentado.

8.4 Prueba PR-02: Enrutado entre VLANs

La siguiente prueba consiste en verificar que la tabla de enrutamiento entre VLANs está bien configurada. El comando “show ip route” efectivamente demuestra que existe una entrada por cada VLAN.

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.239.128.4 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 8 subnets
C       10.239.128.0 is directly connected, GigabitEthernet0/23
C       10.239.69.0 is directly connected, Vlan6
C       10.239.68.0 is directly connected, Vlan5
C       10.239.71.0 is directly connected, Vlan8
C       10.239.70.0 is directly connected, Vlan7
C       10.239.65.0 is directly connected, Vlan2
C       10.239.67.0 is directly connected, Vlan4
C       10.239.66.0 is directly connected, Vlan3
S*   0.0.0.0/0 [1/0] via 10.239.128.4
```

Figura 8-5 Tablas de enrutamiento entre VLANs

8.5 Prueba PR-03: Comprobación del Puente Raíz

Esta prueba consiste en verificar que la configuración del puente raíz es correcta y que por tanto el puente raíz es el switch ScSwitch01. En la siguiente figura se muestra la salida del comando “show spanning-tree”, donde se puede observar que así es.

```
ScSwitch01#show spanning-tree


VLAN0002
  Spanning tree enabled protocol rstp
  Root ID     Priority    2
              Address     0013.1a66.eb80
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    2      (priority 0 sys-id-ext 2)
              Address     0013.1a66.eb80
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Fa0/12              Desg FWD 19        128.12   P2p
```

Figura 8-6 Verificación de que el ScSwitch01 es Puente Raíz

8.6 Prueba PR-04: Aislamiento entre VLAN

La siguiente prueba consiste en verificar que las listas de control de acceso están bien configuradas y que por tanto no es posible acceder desde una VLAN de usuario a otra, a menos que sea la VLAN de informática.

Para demostrarlo, un equipo de Bilbao intenta hacer ping a un equipo de O'Donell y como se puede observar no hay respuesta. El mismo equipo de Bilbao lanza un ping a un equipo de la VLAN de informática y sin embargo en este caso obtiene respuesta.

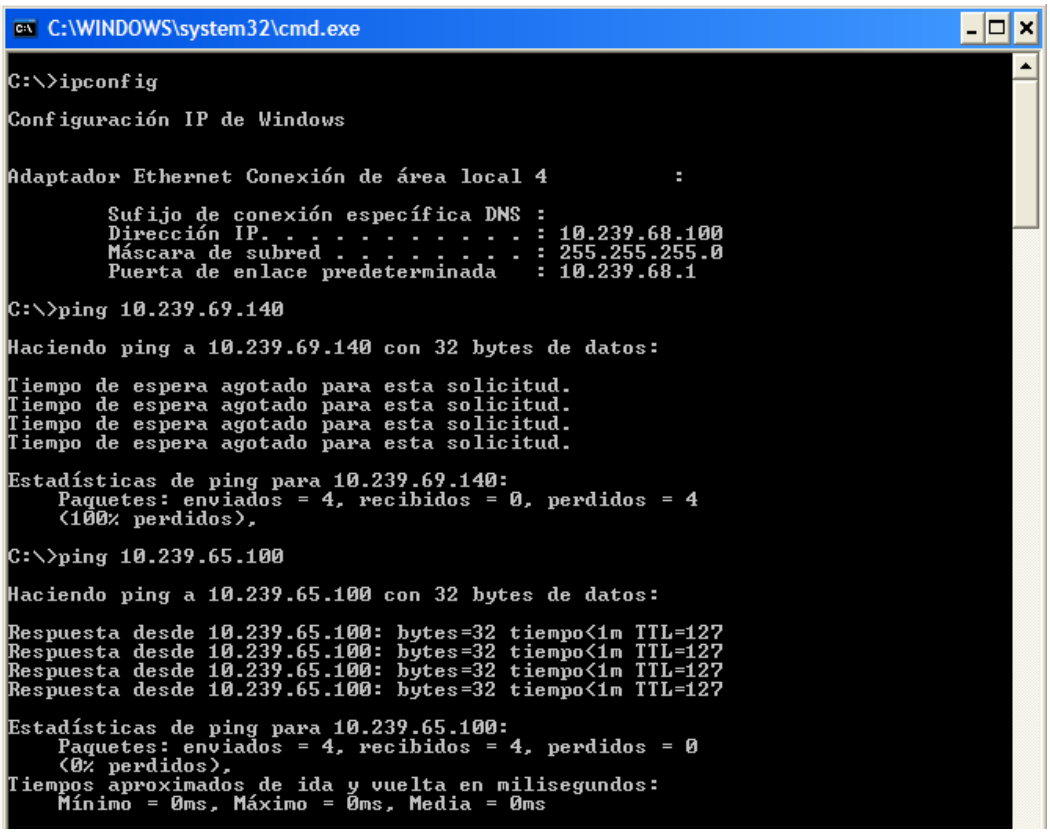


Figura 8-7 Aislamiento entre VLANs

8.7 Prueba PR-05: Seguridad en el acceso a los switches

Esta prueba consiste en verificar que el acceso a los switches solo es permitido a la VLAN de informática. Para ello, se intenta la conexión por ssh desde un equipo de la VLAN de Bilbao al switch ScSwitch01, el resultado es un mensaje de error en la conexión.

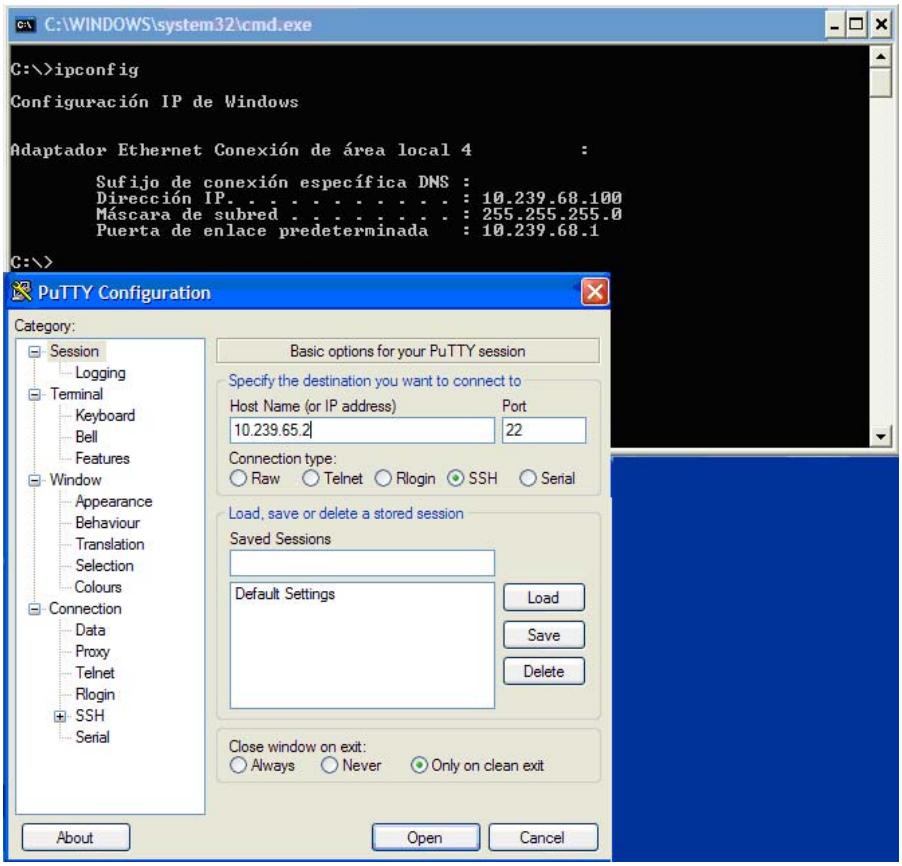


Figura 8-8 Intento de conexión ssh

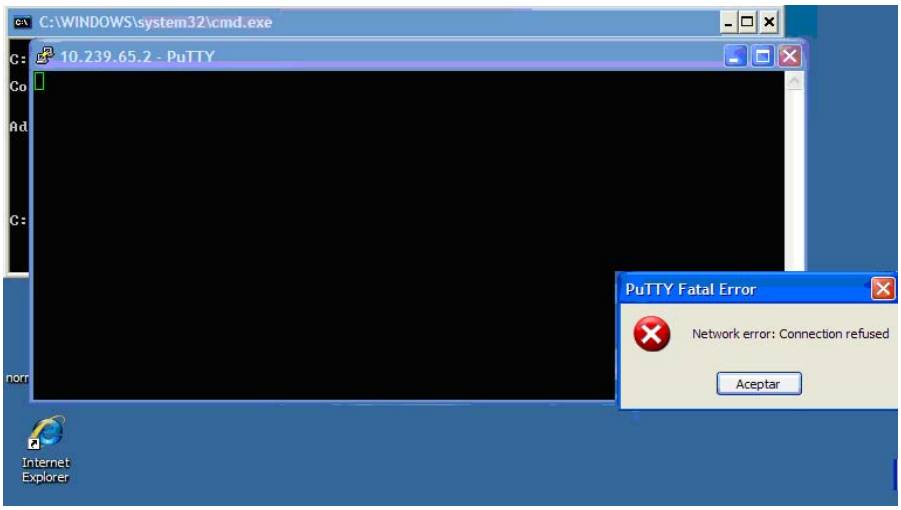


Figura 8-9 Rechazo del intento de conexión

8.8 Prueba PR-06: Alta disponibilidad en capa 2

La siguiente prueba consiste en verificar que la pérdida de conectividad en caso de fallo en uno de los enlaces de un switch, es casi nula. Para ello, se desconecta el cable de red que une el ScSwitch14 al ScSwitch01. Tras unos segundos la conexión se recupera gracias a la redundancia en capa 2.

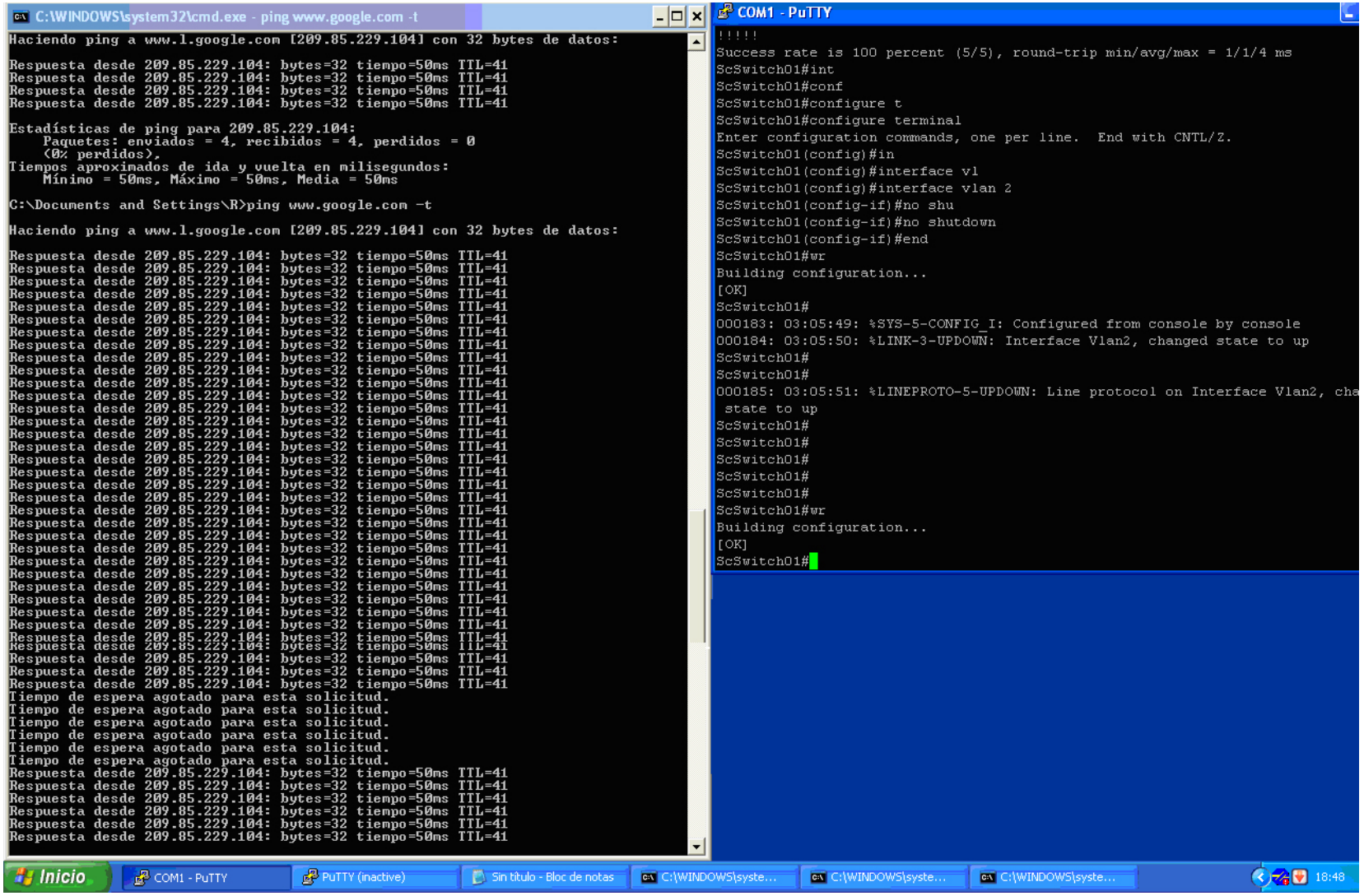


Figura 8-10 Alta disponibilidad en capa 2

8.9 Prueba PR-07: Alta disponibilidad en capa 3 e Interfaz de Tracking

Esta prueba consiste en verificar que la caída del ScSwitch01 provoca una perdida mínima del servicio. Para ello, primero hay que verificar que el ScSwitch01 es el router activo.

```
ScSwitch01#show stand
ScSwitch01#show standby
Vlan2 - Group 2
  State is Active
    4 state changes, last state change 00:30:28
  Virtual IP address is 10.239.65.1
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.440 secs
  Preemption enabled
  Active router is local
  Standby router is 10.239.65.3, priority 100 (expires in 9.440 sec)
  Priority 200 (configured 200)
  Group name is "hsrp-Vl2-2" (default)
Vlan3 - Group 3
  State is Active
    4 state changes, last state change 00:30:28
  Virtual IP address is 10.239.66.1
  Active virtual MAC address is 0000.0c07.ac03
    Local virtual MAC address is 0000.0c07.ac03 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.144 secs
  Preemption enabled
  Active router is local
  Standby router is 10.239.66.3, priority 100 (expires in 7.888 sec)
  Priority 200 (configured 200)
  Group name is "hsrp-Vl3-3" (default)
Vlan4 - Group 4
  State is Active
    4 state changes, last state change 00:30:30
  Virtual IP address is 10.239.67.1
  Active virtual MAC address is 0000.0c07.ac04
    Local virtual MAC address is 0000.0c07.ac04 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.368 secs
  Preemption enabled
  Active router is local
  Standby router is 10.239.67.3, priority 100 (expires in 9.600 sec)
  Priority 200 (configured 200)
  Group name is "hsrp-Vl4-4" (default)
Vlan5 - Group 5
  State is Active
    4 state changes, last state change 00:30:20
  Virtual IP address is 10.239.68.1
  Active virtual MAC address is 0000.0c07.ac05
    Local virtual MAC address is 0000.0c07.ac05 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.240 secs
  Preemption enabled
  Active router is local
  Standby router is 10.239.68.3, priority 100 (expires in 8.800 sec)
  Priority 200 (configured 200)
  Group name is "hsrp-Vl5-5" (default)
Vlan6 - Group 6
  State is Active
    4 state changes, last state change 00:30:31
  Virtual IP address is 10.239.69.1
  Active virtual MAC address is 0000.0c07.ac06
 --More--
```

Figura 8-11 ScSwitch01 es el router activo

El siguiente paso consiste en apagar el ScSwitch01. En las siguientes graficas se muestra como tras unos segundos la conexión se recupera gracias a la redundancia en capa 3.

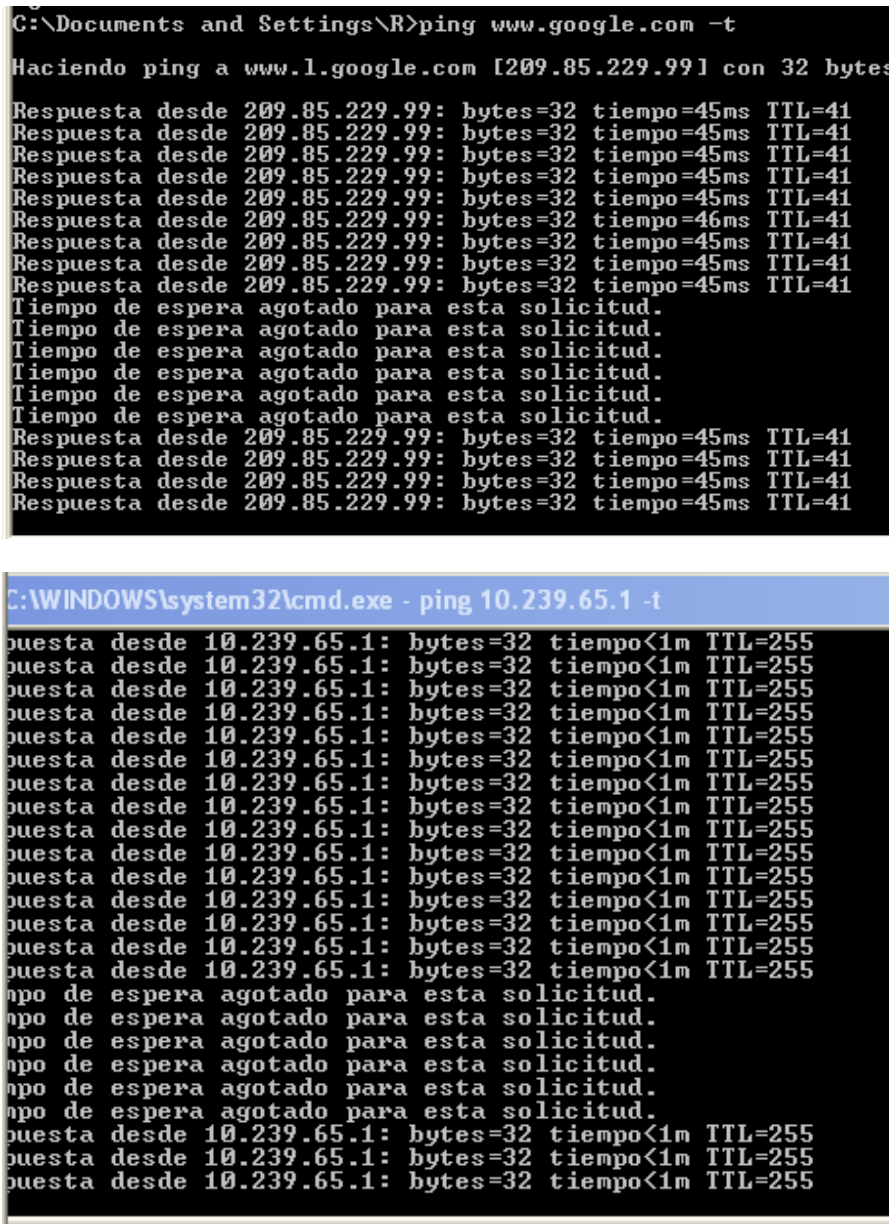


Figura 8-12 Alta disponibilidad en capa 3

Para finalizar las pruebas de HSRP, se procede a desconectar la interfaz de tracking. Como se puede observar en la Figura 8-14, una vez más, la perdida de conectividad es mínima.

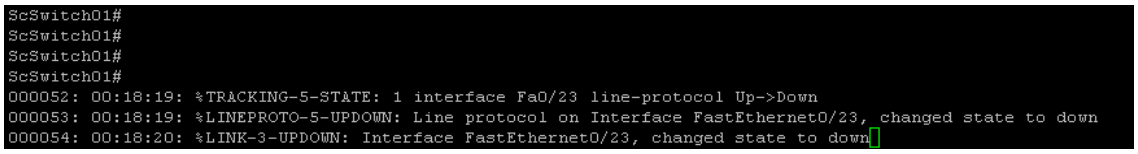


Figura 8-13 Caída interfaz de tracking del switch principal

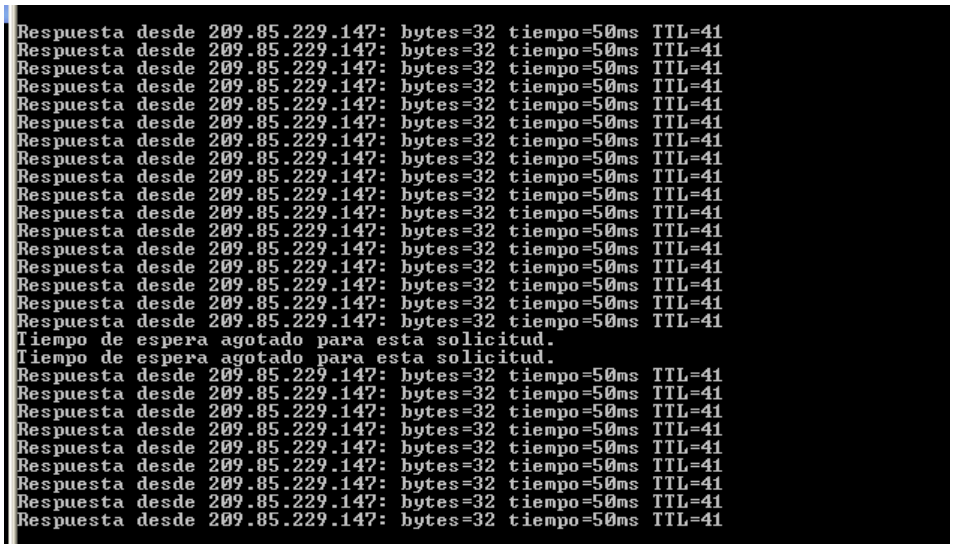


Figura 8-14 Recuperación del servicio tras caída de la interfaz de tracking

8.10 Prueba PR-08: Asignación de IP por DHCP

La siguiente prueba consiste en verificar el correcto funcionamiento del DHCP. Los usuarios obtendrán una IP siempre que su MAC esté dada de alta en el DHCP. Para demostrar que así es, se da de alta a una MAC en el DHCP. La Figura 8-16 refleja que el equipo registrado ha obtenido una IP por medio del DHCP.

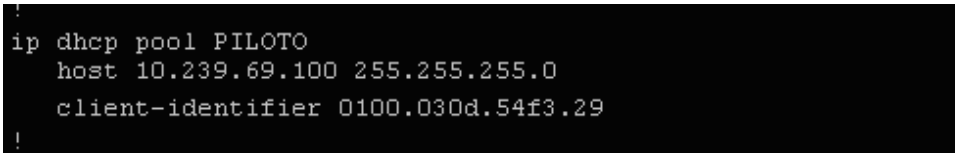


Figura 8-15 Dar de alta a una MAC en el DHCP

Figura 8-16 Obtención de la IP

8.11 Fotografías del entorno de simulación

En este punto se recogen algunas fotos del entorno de simulación montando en el laboratorio. Como se comentó al comienzo del capítulo, por motivos de privacidad de la empresa resulta imposible aportar fotos del entorno real.

La Figura 8-17 muestra el armario de comunicaciones utilizado para simular un entorno de pruebas entre las VLANs de Muñoz Olivé y O'Donell, con salida a la red corporativa.

Figura 8-17 Armario de comunicaciones en laboratorio

Figura 8-18 Entorno de simulación O'Donell

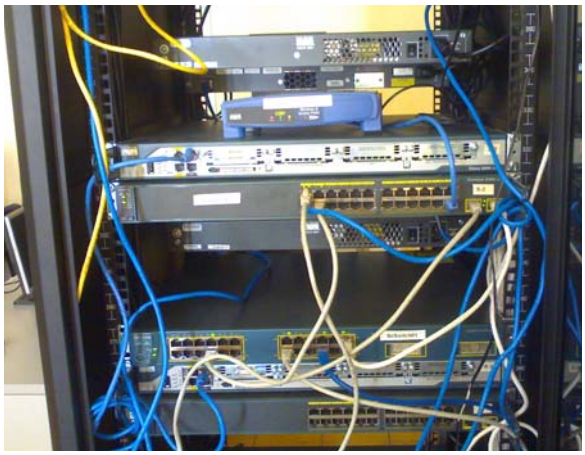


Figura 8-19 Entorno de simulación. Entrada a Muñoz Olivé

8.12 Conclusiones

Todas las pruebas realizadas a la red una vez ésta ha sido puesta en marcha han certificado su correcto funcionamiento. Este capítulo solo ha descrito un pequeño conjunto de las pruebas más significativas, pero aclarar que una batería de pruebas mucho más intensa ha sido ejecutada sobre cada uno de los switches, para demostrar al cliente que la configuración es correcta en cada uno de los entornos definidos Muñoz Olivé, Bilbao y O'Donell.

En cualquier caso, a partir de este momento el IATE cuenta con herramientas para la gestión de la red que facilitan el control y monitorización del estado de los dispositivos, y permiten al administrador actuar ante cualquier incidencia.

Capítulo 9.
Conclusiones y líneas futuras

9.1 Conclusiones finales

En este proyecto fin de carrera se han expuesto los trabajos llevados a cabo en la modernización de la infraestructura de comunicaciones del Instituto Andaluz de la Tercera Edad (IATE) de la Junta de Andalucía, con el fin de adaptar su red a las nuevas tendencias del mercado, persiguiendo aumentar considerablemente su eficiencia y rendimiento.

Surge ante la necesidad de una organización con una estructura de red no jerárquica, que entre otras cosas, impedía la escalabilidad de la misma. Una entidad que presentaba deficiencias importantes, entre las que destacaban alta latencia, colisiones, pérdidas de conectividad, direccionamiento IP ineficiente, bajo rendimiento, falta de mecanismos de seguridad, ausencia de documentación de red, dificultad para la monitorización de errores, y en definitiva, graves obstáculos que dificultaban la actividad cotidiana, tanto de los usuarios como del administrador de la red.

Esta modernización ha supuesto un cambio drástico en la red del IATE, que ha requerido una inversión a largo plazo por parte del cliente y un esfuerzo inicial considerable en el desempeño del administrador de la red, quien ha logrado el objetivo de transicionar de una red no gestionada a una red segura basada en dispositivos gestionables.

Han sido necesarias varias fases para conseguir la puesta en marcha definitiva de una gestión de las comunicaciones mediante una electrónica de red de altas prestaciones que cumpla con los requisitos exigidos.

La elección de los equipos ha conllevado el estudio de diversas tecnologías, aunque finalmente ha sido seleccionada la marca líder del mercado, Cisco, porque las estadísticas demuestran que aunque supone una inversión inicial mayor, reduce los costes operacionales durante el ciclo de vida del producto. Aún así, durante la fase de diseño se han ido elaborando una serie de listas de verificación, las cuales se abstraen de la tecnología empleada, orientadas a resumir las directrices a seguir posteriormente durante la etapa de configuración, momento en el cual se ha hecho uso de los dispositivos Cisco y de su particular sintaxis. Esta división entre teoría y práctica ha sido pensada con el fin de que dichas listas de verificación puedan ser reutilizadas en

caso de ser otra la tecnología seleccionada, aportando, de este modo, un sentido académico a este proyecto fin de carrera.

Durante el desarrollo de las actividades se ha tratado de minimizar el impacto sobre el trabajo diario de los empleados del IATE, por lo que la instalación y configuración de los equipos se ha realizado en fin de semana, periodo en el cual la pérdida del servicio resultaba ser menos crítica para la organización.

La red gestionable, en este caso, implementada mediante switches de alto rendimiento de la familia Cisco Catalyst, ha facilitado la administración, configuración, mantenimiento y resolución de problemas. Y lo que es más, ha convertido a la red del IATE en una red segura, ya que ha aportado seguridad tanto física como lógica, combatiendo los ataques más comunes contra dispositivos de capa 2. Este sentido, el firewall también ha realizado su aportación, proporcionando seguridad perimetral.

Como resultado del uso de la redundancia a nivel de capa 2 y 3, el periodo de inactividad de la red ahora es prácticamente nulo. Por otra parte, destacar la importancia de la gestión de la red, ya que además de reducir el tiempo de respuesta ante la caída del sistema, ha ayudado a identificar problemas con la anticipación suficiente como para evitar que la situación se convierta en una emergencia, manteniendo al tanto en todo momento al administrador de la red sobre el estado de la misma.

Como conclusión final hacer hincapié en que el diseño de una red local no debe dejarse a la improvisación, sino que debe ser el producto de un análisis pormenorizado de las necesidades requeridas por la empresa en cuestión, y tiene que seguir una serie de criterios de calidad y funcionalidad mínimos a la hora de su implementación o instalación física, con el fin de alcanzar una red estable, fiable, segura y escalable. Descuidar tales factores desembocaría sin duda en situaciones de error o mal funcionamiento, convirtiéndose en un freno para la actividad de la empresa y, consecuentemente, en una pérdida de los niveles de eficiencia. Elegir la mejor electrónica de red y la mejor solución de conectividad en función de las necesidades de la empresa es de crucial importancia para el rendimiento de la misma. Todo ello sin olvidar que el diseño debe ser adaptable, por lo que no debe incluir elementos que puedan limitar la implementación de nuevas tecnologías

El presente proyecto es la base de una línea de trabajo que se pretende continuar con el mantenimiento y mejora continúa de la red del IATE.

9.2 Líneas futuras

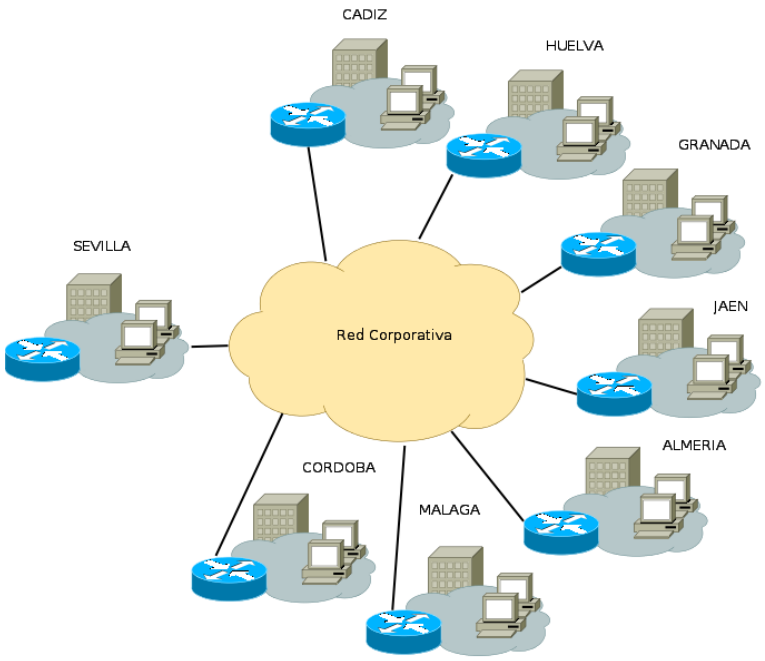
Para finalizar este documento se proponen una serie de mejoras que se podrían aplicar a este proyecto fin de carrera, enfocadas en cuatro vertientes:

- Creación de las futuras direcciones provinciales
- Incrementar la seguridad en la red cableada
- Mejoras en la Red Wireless Interna y Externa
- Implementación de IDS/IPS/Honeypot en la DMZ.

9.2.1 Creación de las futuras direcciones provinciales

Como ya se ha comentó en el primer capitulo, debido a la aceptación que están teniendo los servicios que ofrece el IATE y a la creciente demanda originada en otras provincias Andaluzas, está previsto en un plazo de 2 años la creación progresiva de diferentes delegaciones provinciales (DD.PP.), cuyas sedes estarían distribuidas por el resto de Andalucía. Por tanto, una línea de trabajo ineludible sería el despliegue y puesta en marcha de la red completa, así como las pertinentes pruebas para la comprobación de su correcto funcionamiento.

La siguiente figura muestra el diseño lógico de la futura red corporativa del IATE, donde se refleja que cada DD.PP se conecta a SS.CC.



LOCALIZACIÓN	TIPO	OBSERVACIÓN
Sevilla - Olivé	Sede principal	Ubicación de servidores principales
Sevilla - O'Donnell	Oficina	Se conecta a SS.CC.
Sevilla - Bilbao	Oficina	Se conecta a SS.CC.
Cádiz	Oficina	Se conecta a SS.CC.
Huelva	Oficina	Se conecta a SS.CC.
Málaga	Oficina	Se conecta a SS.CC.
Córdoba	Oficina	Se conecta a SS.CC.
Granada	Oficina	Se conecta a SS.CC.
Jaén	Oficina	Se conecta a SS.CC.
Almería	Oficina	Se conecta a SS.CC.

Figura 9- 1 Diseño lógico de la futura red del IATE

La modernización a la que se ha visto sometida los SS.CC del IATE durante el desarrollo del presente proyecto fin de carrera, ha sido realizada teniendo presente en todo momento que la sede de Sevilla debe esté preparada para dar soporte al resto de delegaciones cuando se produzca la expansión. Incluso con el fin de ir avanzando los trabajos en este sentido, se ha calculado el direccionamiento previsto para las futuras DD.PP. y los resultados se han incluido en el anexo D de este documento.

9.2.2 Incrementar la seguridad en la red cableada

Como un paso más en la seguridad cableada, una mejora a considerar podría ser implementar CISCO IBNS (Identity Based Network Services).

IBNS combina switches Catalyst, dispositivos WLAN y servidores RADIUS para ofrecer autentificación, control de acceso y políticas de usuario para asegurar la conectividad de la red y los recursos. Autentica usuarios individuales y/o dispositivos, y tras la autenticación, un permiso a un usuario o dispositivo puede ser controlado mediante una política configurada.

9.2.3 Mejoras en la Red Wireless Interna y Externa

Si en el futuro el cliente estuviera dispuesto a realizar una mayor inversión en la infraestructura de la red inalámbrica, para la Wireless externa sería interesante adquirir puentes inalámbricos que soporten 802.1q. Esto permitiría extender las VLAN, además de crear redundancia usando dos puentes inalámbricos por sede. De este modo se obtendría alta disponibilidad en toda la red.

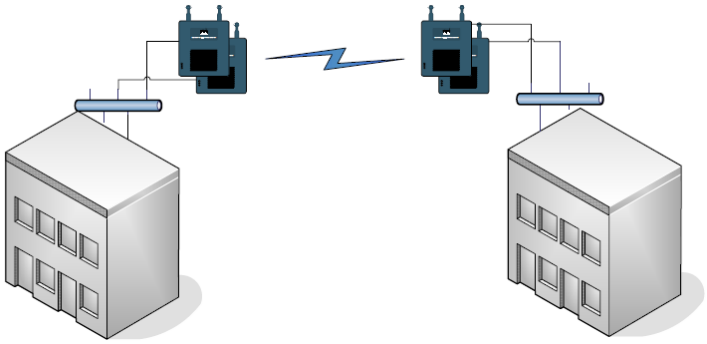


Figura 9- 2 Mejora en la Red Wireless Externa de SS.CC.

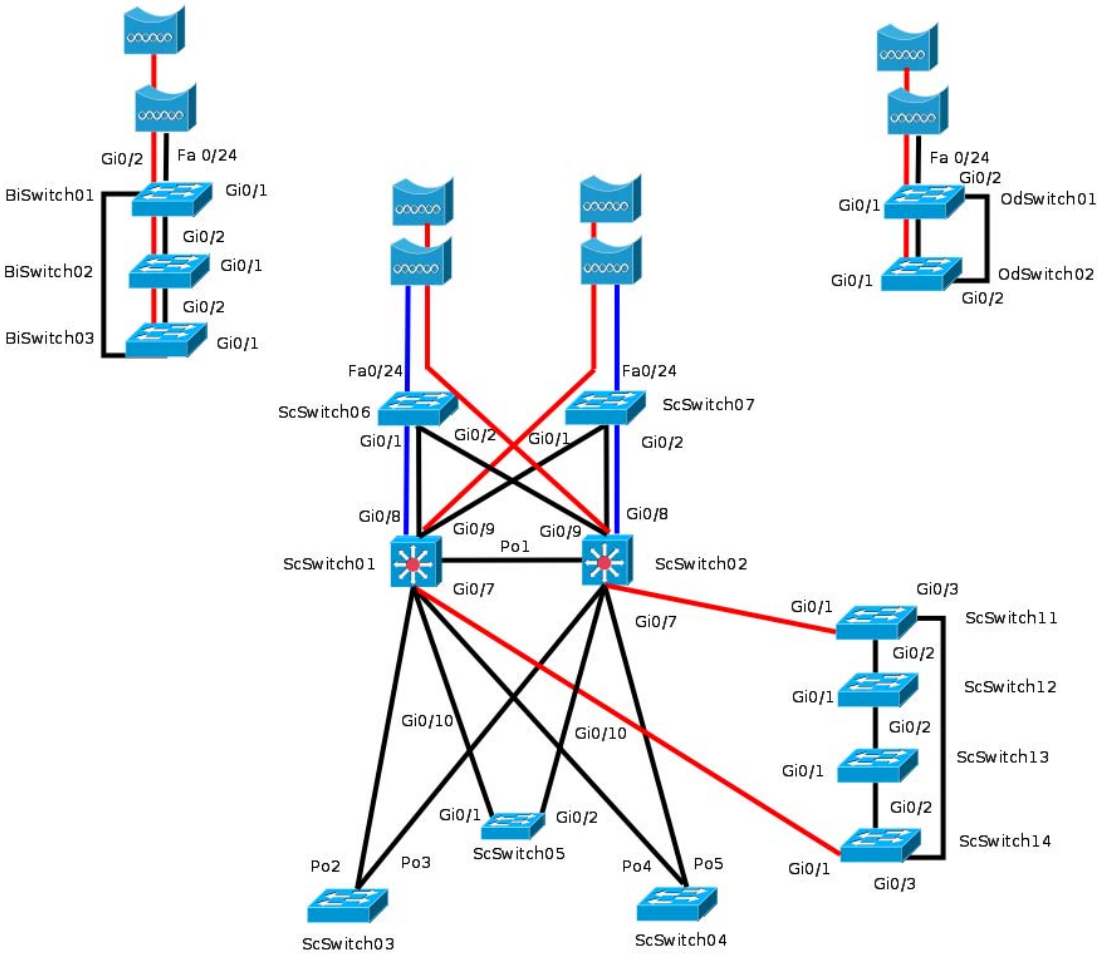


Figura 9- 3 Mejora en Wireless Externa que permite alta disponibilidad

Respecto a la Wireless interna se podría emplear Wireless Lan Controller junto a puntos de acceso del tipo Lightweight, simplificando la implementación y operación de las redes inalámbricas.

9.2.4 Implementación de IDS/IPS/Honeypot en la DMZ

Una última línea futura bastante interesante podría ser la implementación de Sistemas de Detección de Intrusos (IDS) y/o Sistemas de Prevención de Intrusos (IPS) en la zona desmilitarizada o DMZ.

Los IDS detectan las posibles causas, fallos o vulnerabilidades de la red e informan al administrador. Mientras que los IPS son dispositivos que ejercen el control de acceso en una red, para proteger a los sistemas computacionales de ataques y abusos. La tecnología de Prevención de Intrusos es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos, pero en realidad no es más que otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.

Los IPS presentan una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basadas en los contenidos del tráfico, en lugar de en direcciones IP o puertos, e incluso pueden actuar a nivel de equipo, para combatir actividades potencialmente maliciosas.

Además de los IDS e IPS, otra opción a tener en cuenta podría ser la instalación de honeypot, que se definen como software o conjunto de computadores cuya intención es atraer a atacantes, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas. Los Honeypots pueden distraer a los atacantes de las máquinas más importantes del sistema, y advertir rápidamente al administrador del sistema de un ataque, además de permitir un examen en profundidad del atacante, durante y después del ataque al honeypot.

Anexo A. Presupuesto Económico

Modelo	Imagen	Descripción del elemento	Contrato de mantenimiento	Cantidad	Coste Unidad	Coste Total
Cisco Catalyst 2960-24TC-L		24 Ethernet 10/100/1000 2 puertos Dual-purpose a 10/100/1000	3 años	15	1400 €	21000 €
Cisco Catalyst 2960-S-24TS-L		24 Ethernet 10/100/1000 4 puertos Dual-purpose a 1 Gb	3 años	3	1500 €	4500 €
Cisco Catalyst 2960G-24TC-L		20 Ethernet 10/100/1000 4 puertos Dual-purpose a 10/100/1000	3 años	3	2500 €	7500 €
Cisco Catalyst 3560G-24TS		24 Ethernet 10/100/1000 4 SFP-Gigabit Ethernet ports	3 años	3	3600 €	10800 €
Conectores SFP GLC-SX-MM		Conector de interconexión	3 años	16	300 €	4800 €
Cables de fibra LC-ST		Cables de interconexión	N/A	16	35 €	560 €
Wireless Externa	N/A	Trabajos realizados por empresa externa	3 años	4 puentes + Instalación	N/A	3000 €
					TOTAL	52.160 €

Tabla A- 1 Presupuesto Económico

Anexo B. Hardware Empleado

B.1 Introducción

En este anexo recoge las especificaciones técnicas de los dispositivos empleados en el presente proyecto fin de carrera.

B.2 Switch Cisco Catalyst 2960

Data Sheet - Cisco 2960

B.3 Switch Cisco Catalyst 3560

Data Sheet - Cisco 3560

B.4 Punto de acceso inalámbrico Linksys WAP54G v.2

Linksys WAP54G v.2

Anexo C. Documentación de la red.

C.1 Introducción

Este anexo consiste en un documento Excel que recopila todas las tablas que incluyen la documentación de la red del IATE. Dada la extensión del mismo no resulta práctico incluirlo en los tomos impresos, pero puede ser localizado en el DVD junto con al resto de la documentación de este proyecto fin de carrera.

- Tabla C-1 Administración
- Tabla C-2 Servidores (VLAN 4- DMZ)
- Tabla C-3 SAI
- Tabla C-4 Informática (VLAN 2)
- Tabla C-5 Impresoras
- Tabla C-6 Equipos Usuarios (VLAN3,5,6)
- Tabla C-7 CPD
- Tabla C-8 Pasillo
- Tabla C-9 Bilbao
- Tabla C-10 O'Donell
- Tabla C-11 DMZ
- Tabla C-12 ScSwitch01
- Tabla C-13 ScSwitch02
- Tabla C-14 ScSwitch03
- Tabla C-15 ScSwitch04
- Tabla C-16 ScSwitch05
- Tabla C-17 ScSwitch06
- Tabla C-18 ScSwitch07
- Tabla C-19 ScSwitch11
- Tabla C-20 ScSwitch12
- Tabla C-21 ScSwitch13
- Tabla C-22 ScSwitch14
- Tabla C-23 BiSwitch01
- Tabla C-24 BiSwitch02
- Tabla C-25 BiSwitch03
- Tabla C-26 OdSwitch01
- Tabla C-27 OdSwitch02

Nombre del dispositivo	Sistema operativo	IP	Mascara Subred	Estática/ Dinámica	VLAN
IP HSRP VLAN 8	IOS	10.239.71.1	255.255.255.0	Estática	VLAN 8
ScSwitch01	IOS	10.239.71.2	255.255.255.0	Estática	VLAN 8
ScSwitch02	IOS	10.239.71.3	255.255.255.0	Estática	VLAN 8
ScSwitch03	IOS	10.239.71.103	255.255.255.0	Estática	VLAN 8
ScSwitch04	IOS	10.239.71.104	255.255.255.0	Estática	VLAN 8
ScSwitch05	IOS	10.239.71.105	255.255.255.0	Estática	VLAN 8
ScSwitch06	IOS	10.239.71.106	255.255.255.0	Estática	VLAN 8
ScSwitch07	IOS	10.239.71.107	255.255.255.0	Estática	VLAN 8
ScSwitch11	IOS	10.239.71.111	255.255.255.0	Estática	VLAN 8
ScSwitch12	IOS	10.239.71.112	255.255.255.0	Estática	VLAN 8
ScSwitch13	IOS	10.239.71.113	255.255.255.0	Estática	VLAN 8
ScSwitch14	IOS	10.239.71.114	255.255.255.0	Estática	VLAN 8
ScExterno	IOS	10.239.71.115	255.255.255.0	Estática	VLAN 8
PuenteSscc-Bilbao	IOS	10.239.68.253	255.255.255.0	Estática	VLAN 5
PuenteSscc-Odonell	IOS	10.239.69.253	255.255.255.0	Estática	VLAN 6
PuenteBilbao	IOS	10.239.68.254	255.255.255.0	Estática	VLAN 5
PuenteOdonell	IOS	10.239.69.254	255.255.255.0	Estática	VLAN 6
BiSwitch01	IOS	10.239.68.241	255.255.255.0	Estática	VLAN 5
BiSwitch02	IOS	10.239.68.242	255.255.255.0	Estática	VLAN 5
BiSwitch03	IOS	10.239.68.243	255.255.255.0	Estática	VLAN 5
OdSwitch01	IOS	10.239.69.241	255.255.255.0	Estática	VLAN 6
OdSwitch01	IOS	10.239.69.242	255.255.255.0	Estática	VLAN 6

Tabla C-1 Administración

Nombre del dispositivo	Sistema operativo	IP	Mascara Subred	Estatica/ Dinamica	VLAN
IP CLUSTER DMZ	Linux	10.239.64.1	255.255.255.0	Estática	DMZ
Cervero1 (Firewall1)	Linux	10.239.64.2	255.255.255.0	Estática	DMZ
Cervero2 (Firewall2)	Linux	10.239.64.3	255.255.255.0	Estática	DMZ
SwitchDMZ	IOS	10.239.64.10	255.255.255.0	Estática	DMZ
Hades (Webserver)	Linux	10.239.64.16	255.255.255.0	Estática	DMZ
IP HSRP VLAN 4	IOS	10.239.67.1	255.255.255.0	Estática	VLAN 4
ScSwitch01	IOS	10.239.67.2	255.255.255.0	Estatica	VLAN 4
ScSwitch02	IOS	10.239.67.3	255.255.255.0	Estática	VLAN 4
Neptuno (DBServer1)	Linux	10.239.67.100	255.255.255.0	Estática	VLAN 4
Hefesto (Webinterno)	Linux	10.239.67.101	255.255.255.0	Estática	VLAN 4
Desarrollo1	Linux	10.239.67.102	255.255.255.0	Estática	VLAN 4
Desarrollo2	Linux	10.239.67.103	255.255.255.0	Estática	VLAN 4
Poseidon (DBServer2)	Linux	10.239.67.104	255.255.255.0	Estática	VLAN 4
Atenea1 (Proxy)	Linux	10.239.67.105	255.255.255.0	Estática	VLAN 4
Atenea2 (DNS)	Linux	10.239.67.106	255.255.255.0	Estática	VLAN 4
Afrodita(Dominio1)	Linux	10.239.67.107	255.255.255.0	Estática	VLAN 4
Helios(Monitorizacion)	Linux	10.239.67.108	255.255.255.0	Estática	VLAN 4
Apolo (Servidor Impresion)	Windows 2003	10.239.67.109	255.255.255.0	Estática	VLAN 4
Backup	Windows 2003	10.239.67.110	255.255.255.0	Estática	VLAN 4

Tabla C-2 Servidores (VLAN 4 - DMZ)

SAI	IP/Mascara	VLAN
Sai01	10.239.67.251	VLAN 4
Sai02	10.239.67.252	VLAN 4
Sai03	10.239.67.253	VLAN 4
Sai04	10.239.66.254	VLAN 3
BiSai01	10.239.68.251	VLAN 5
OdSai01	10.239.69.251	VLAN 6

Tabla C-3 SAI

Nombre del dispositivo	Sistema operativo	IP	Mascara Subred	Estatica/ Dinamica	VLAN	Libre
INF100	Linux	10.239.65.100	255.255.255.0	Estática	2	NO
INF101	Linux	10.239.65.101	255.255.255.0	Estática	2	NO
INF102	Windows XP	10.239.65.102	255.255.255.0	Dinámica	2	NO
INF103	Windows XP	10.239.65.103	255.255.255.0	Dinámica	2	NO
INF104	Windows XP	10.239.65.104	255.255.255.0	Dinámica	2	NO
INF105	Windows XP	10.239.65.105	255.255.255.0	Dinámica	2	NO
INF106	Windows XP	10.239.65.106	255.255.255.0	Dinámica	2	NO
INF107	Windows XP	10.239.65.107	255.255.255.0	Dinámica	2	NO
INF108	Windows XP	10.239.65.108	255.255.255.0	Dinámica	2	NO
INF109	Windows XP	10.239.65.109	255.255.255.0	Dinámica	2	NO
INF110	Windows XP	10.239.65.110	255.255.255.0	Dinámica	2	NO
PORIAJ11	Windows XP	10.239.65.111	255.255.255.0	Dinámica	2	NO
PORIAJ12	Windows XP	10.239.65.112	255.255.255.0	Dinámica	2	NO
PORIAJ13	Windows XP	10.239.65.113	255.255.255.0	Dinámica	2	NO
PORIAJ14	Windows XP	10.239.65.114	255.255.255.0	Dinámica	2	NO
PORIAJ15	Windows XP	10.239.65.115	255.255.255.0	Dinámica	2	NO
PORIAJ16	Windows XP	10.239.65.116	255.255.255.0	Dinámica	2	NO
PRUEBAS	Windows XP	10.239.65.117	255.255.255.0	Dinámica	2	NO
INF118	-----	10.239.65.118	-----	-----	-----	SI
INF119	-----	10.239.65.119	-----	-----	-----	SI
INF120	-----	10.239.65.120	-----	-----	-----	SI

Tabla C-4 Informática (VLAN 2)

Nombre del dispositivo	IP	Mascara Subred	Estatica/Dinamica	VLAN
Konica Minolta	10.239.65.200	255.255.255.0	Estatica	2
Konica Minolta	10.239.65.201	255.255.255.0	Estatica	2
Konica Minolta	10.239.66.200	255.255.255.0	Estatica	3
Konica Minolta	10.239.66.201	255.255.255.0	Estatica	3
Konica Minolta	10.239.66.202	255.255.255.0	Estatica	3
Konica Minolta	10.239.66.203	255.255.255.0	Estatica	3
Konica Minolta	10.239.66.204	255.255.255.0	Estatica	3
Konica Minolta	10.239.66.205	255.255.255.0	Estatica	3
Konica Minolta	10.239.66.206	255.255.255.0	Estatica	3
Gestener	10.239.66.207	255.255.255.0	Estatica	3
Gestener	10.239.66.208	255.255.255.0	Estatica	3
Konica Minolta	10.239.68.200	255.255.255.0	Estatica	5
Konica Minolta	10.239.68.201	255.255.255.0	Estatica	5
Konica Minolta	10.239.68.202	255.255.255.0	Estatica	5
Konica Minolta	10.239.68.203	255.255.255.0	Estatica	5
Konica Minolta	10.239.68.204	255.255.255.0	Estatica	5
Konica Minolta	10.239.68.205	255.255.255.0	Estatica	5
Gestener	10.239.68.206	255.255.255.0	Estatica	5
Gestener	10.239.68.207	255.255.255.0	Estatica	5
Gestener	10.239.68.208	255.255.255.0	Estatica	5
Gestener	10.239.68.209	255.255.255.0	Estatica	5
Konica Minolta	10.239.69.200	255.255.255.0	Estatica	5
Konica Minolta	10.239.69.201	255.255.255.0	Estatica	6
Konica Minolta	10.239.69.202	255.255.255.0	Estatica	6
Gestener	10.239.69.203	255.255.255.0	Estatica	6
Gestener	10.239.69.204	255.255.255.0	Estatica	6

Tabla C-5 Impresoras

Nombre del dispositivo	Sistema operativo	IP	Mascara Subred	Estatica/ Dinamica	VLAN	Libre
HSRP Catalyst 3560	IOS	10.239.66.1	255.255.255.0	Estática	3	No
ScSwitch01	Windows 2000	10.239.66.2	255.255.255.0	Estática	3	No
ScSwitch02	Windows 2000	10.239.66.3	255.255.255.0	Estática	3	No
SSCC004	Windows 2000	10.239.66.4	255.255.255.0	Dinámica	3	No
SSCC005	Windows XP	10.239.66.5	255.255.255.0	Dinámica	3	No
SSCC006	Windows XP	10.239.66.6	255.255.255.0	Dinámica	3	No
SSCC007	Windows XP	10.239.66.7	255.255.255.0	Dinámica	3	No
SSCC008	Windows XP	10.239.66.8	255.255.255.0	Dinámica	3	No
SSCC009	Windows XP	10.239.66.9	255.255.255.0	Dinámica	3	No
SSCC010	Windows XP	10.239.66.10	255.255.255.0	Dinámica	3	No
SSCC011	Windows XP	10.239.66.11	255.255.255.0	Dinámica	3	No
SSCC012	Windows 2000	10.239.66.12	255.255.255.0	Dinámica	3	No
SSCC013	Windows 2000	10.239.66.13	255.255.255.0	Dinámica	3	No
SSCC014	Windows XP	10.239.66.14	255.255.255.0	Dinámica	3	No
SSCC015	Windows XP	10.239.66.15	255.255.255.0	Dinámica	3	No
SSCC016	Windows XP	10.239.66.16	255.255.255.0	Dinámica	3	No
SSCC017	Windows XP	10.239.66.17	255.255.255.0	Dinámica	3	No
SSCC018	Windows XP	10.239.66.18	255.255.255.0	Dinámica	3	No
SSCC019	Windows XP	10.239.66.19	255.255.255.0	Dinámica	3	No
SSCC020	Windows 2000	10.239.66.20	255.255.255.0	Dinámica	3	No
SSCC021	Windows XP	10.239.66.21	255.255.255.0	Dinámica	3	No
SSCC022	Windows XP	10.239.66.22	255.255.255.0	Dinámica	3	No
SSCC023	Windows XP	10.239.66.23	255.255.255.0	Dinámica	3	No
SSCC024	Windows XP	10.239.66.24	255.255.255.0	Dinámica	3	No
SSCC025	Windows XP	10.239.66.25	255.255.255.0	Dinámica	3	No
SSCC026	Windows XP	10.239.66.26	255.255.255.0	Dinámica	3	No
SSCC027	Windows XP	10.239.66.27	255.255.255.0	Dinámica	3	No
SSCC028	Windows XP	10.239.66.28	255.255.255.0	Dinámica	3	No
SSCC029	Windows XP	10.239.66.29	255.255.255.0	Dinámica	3	No
SSCC030	Windows XP	10.239.66.30	255.255.255.0	Dinámica	3	No
SSCC031	Windows XP	10.239.66.31	255.255.255.0	Dinámica	3	No

Nombre del dispositivo	Sistema operativo	IP	Mascara Subred	Estatica/ Dinamica	VLAN	Libre
SSCC032	Windows XP	10.239.66.32	255.255.255.0	Dinámica	3	No
SSCC033	Windows XP	10.239.66.33	255.255.255.0	Dinámica	3	No
SSCC034	Windows 2000	10.239.66.34	255.255.255.0	Dinámica	3	No
SSCC035	Windows 2000	10.239.66.35	255.255.255.0	Dinámica	3	No
SSCC036	Windows 2000	10.239.66.36	255.255.255.0	Dinámica	3	No
SSCC037	Windows 2000	10.239.66.37	255.255.255.0	Dinámica	3	No
SSCC038	Windows 2000	10.239.66.38	255.255.255.0	Dinámica	3	No
SSCC039	Windows 2000	10.239.66.39	255.255.255.0	Dinámica	3	No
SSCC040	Windows 2000	10.239.66.40	255.255.255.0	Dinámica	3	No
SSCC041	Windows 2000	10.239.66.41	255.255.255.0	Dinámica	3	No
SSCC042	Windows 2000	10.239.66.42	255.255.255.0	Dinámica	3	No
SSCC043	Windows 2000	10.239.66.43	255.255.255.0	Dinámica	3	No
SSCC044	Windows 2000	10.239.66.44	255.255.255.0	Dinámica	3	No
SSCC045	Windows 2000	10.239.66.45	255.255.255.0	Dinámica	3	No
SSCC046	Windows 2000	10.239.66.46	255.255.255.0	Dinámica	3	No
SSCC047	Windows 2000	10.239.66.47	255.255.255.0	Dinámica	3	No
SSCC048	Windows 2000	10.239.66.48	255.255.255.0	Dinámica	3	No
SSCC049	Windows 2000	10.239.66.49	255.255.255.0	Dinámica	3	No
SSCC050	Windows 2000	10.239.66.50	255.255.255.0	Dinámica	3	No
SSCC051	Windows XP	10.239.66.51	255.255.255.0	Dinámica	3	No
SSCC052	Windows XP	10.239.66.52	255.255.255.0	Dinámica	3	No
SSCC053	Windows XP	10.239.66.53	255.255.255.0	Dinámica	3	No
SSCC054	Windows XP	10.239.66.54	255.255.255.0	Dinámica	3	No
SSCC055	Windows XP	10.239.66.55	255.255.255.0	Dinámica	3	No
SSCC056	Windows XP	10.239.66.56	255.255.255.0	Dinámica	3	No
SSCC057	Windows XP	10.239.66.57	255.255.255.0	Dinámica	3	No
SSCC058	Windows XP	10.239.66.58	255.255.255.0	Dinámica	3	No
SSCC059	Windows XP	10.239.66.59	255.255.255.0	Dinámica	3	No
SSCC060	Windows XP	10.239.66.60	255.255.255.0	Dinámica	3	No
SSCC061	Windows XP	10.239.66.61	255.255.255.0	Dinámica	3	No
SSCC062	Windows XP	10.239.66.62	255.255.255.0	Dinámica	3	No

Nombre del dispositivo	Sistema operativo	IP	Mascara Subred	Estatica/ Dinamica	VLAN	Libre
SSCC063	-----	10.239.66.63	255.255.255.0	-----	3	SI
SSCC064	-----	10.239.66.64	255.255.255.0	-----	3	SI
SSCC065	-----	10.239.66.65	255.255.255.0	-----	3	SI
SSCC066	-----	10.239.66.66	255.255.255.0	-----	3	SI
SSCC067	-----	10.239.66.67	255.255.255.0	-----	3	SI
SSCC068	-----	10.239.66.68	255.255.255.0	-----	3	SI
SSCC069	-----	10.239.66.69	255.255.255.0	-----	3	SI
SSCC070	Windows 2000	10.239.68.70	255.255.255.0	Dinámica	3	No
SSCC071	Windows 2000	10.239.68.71	255.255.255.0	Dinámica	5	No
SSCC072	Windows 2000	10.239.68.72	255.255.255.0	Dinámica	5	No
SSCC073	Windows 2000	10.239.68.73	255.255.255.0	Dinámica	5	No
SSCC074	Windows 2000	10.239.68.74	255.255.255.0	Dinámica	5	No
SSCC075	Windows 2000	10.239.68.75	255.255.255.0	Dinámica	5	No
SSCC076	Windows 2000	10.239.68.76	255.255.255.0	Dinámica	5	No
SSCC077	Windows 2000	10.239.68.77	255.255.255.0	Dinámica	5	No
SSCC078	Windows 2000	10.239.68.78	255.255.255.0	Dinámica	5	No
SSCC079	Windows 2000	10.239.68.79	255.255.255.0	Dinámica	5	No
SSCC080	Windows 2000	10.239.68.80	255.255.255.0	Dinámica	5	No
SSCC081	Windows 2000	10.239.68.81	255.255.255.0	Dinámica	5	No
SSCC082	Windows 2000	10.239.68.82	255.255.255.0	Dinámica	5	No
SSCC083	Windows 2000	10.239.68.83	255.255.255.0	Dinámica	5	No
SSCC084	Windows XP	10.239.68.84	255.255.255.0	Dinámica	5	No
SSCC085	Windows XP	10.239.68.85	255.255.255.0	Dinámica	5	No
SSCC086	Windows XP	10.239.68.86	255.255.255.0	Dinámica	5	No
SSCC087	Windows XP	10.239.68.87	255.255.255.0	Dinámica	5	No
SSCC088	Windows XP	10.239.68.88	255.255.255.0	Dinámica	5	No
SSCC089	Windows XP	10.239.68.89	255.255.255.0	Dinámica	5	No
SSCC090	Windows XP	10.239.68.90	255.255.255.0	Dinámica	5	No
SSCC091	Windows XP	10.239.68.91	255.255.255.0	Dinámica	5	No
SSCC092	Windows XP	10.239.68.92	255.255.255.0	Dinámica	5	No
SSCC093	Windows XP	10.239.68.93	255.255.255.0	Dinámica	5	No

Nombre del dispositivo	Sistema operativo	IP	Mascara Subred	Estatica/ Dinamica	VLAN	Libre
SSCC094	Windows XP	10.239.68.94	255.255.255.0	Dinámica	5	No
SSCC095	Windows XP	10.239.68.95	255.255.255.0	Dinámica	5	No
SSCC096	Windows XP	10.239.68.96	255.255.255.0	Dinámica	5	No
SSCC097	Windows XP	10.239.68.97	255.255.255.0	Dinámica	5	No
SSCC098	Windows 2000	10.239.68.98	255.255.255.0	Dinámica	5	No
SSCC099	Windows 2000	10.239.68.99	255.255.255.0	Dinámica	5	No
SSCC100	Windows 2000	10.239.68.100	255.255.255.0	Dinámica	5	No
SSCC101	Windows 2000	10.239.68.101	255.255.255.0	Dinámica	5	No
SSCC102	Windows 2000	10.239.68.102	255.255.255.0	Dinámica	5	No
SSCC103	Windows 2000	10.239.68.103	255.255.255.0	Dinámica	5	No
SSCC104	Windows 2000	10.239.68.104	255.255.255.0	Dinámica	5	No
SSCC105	Windows 2000	10.239.68.105	255.255.255.0	Dinámica	5	No
SSCC106	Windows 2000	10.239.68.106	255.255.255.0	Dinámica	5	No
SSCC107	Windows 2000	10.239.68.107	255.255.255.0	Dinámica	5	No
SSCC108	Windows 2000	10.239.68.108	255.255.255.0	Dinámica	5	No
SSCC109	Windows 2000	10.239.68.109	255.255.255.0	Dinámica	5	No
SSCC110	Windows XP	10.239.68.110	255.255.255.0	Dinámica	5	No
SSCC111	Windows XP	10.239.68.111	255.255.255.0	Dinámica	5	No
SSCC112	Windows XP	10.239.68.112	255.255.255.0	Dinámica	5	No
SSCC113	Windows XP	10.239.68.113	255.255.255.0	Dinámica	5	No
SSCC114	Windows XP	10.239.68.114	255.255.255.0	Dinámica	5	No
SSCC115	Windows XP	10.239.68.115	255.255.255.0	Dinámica	5	No
SSCC116	Windows XP	10.239.68.116	255.255.255.0	Dinámica	5	No
SSCC117	Windows XP	10.239.68.117	255.255.255.0	Dinámica	5	No
SSCC118	Windows XP	10.239.68.118	255.255.255.0	Dinámica	5	No
SSCC119	Windows XP	10.239.68.119	255.255.255.0	Dinámica	5	No
SSCC120	Windows XP	10.239.68.120	255.255.255.0	Dinámica	5	No
SSCC121	Windows XP	10.239.68.121	255.255.255.0	Dinámica	5	No
SSCC122	Windows XP	10.239.68.122	255.255.255.0	Dinámica	5	No
SSCC123	Windows XP	10.239.68.123	255.255.255.0	Dinámica	5	No
SSCC124	Windows 2000	10.239.68.124	255.255.255.0	Dinámica	5	No

Nombre del dispositivo	Sistema operativo	IP	Mascara Subred	Estatica/ Dinamica	VLAN	Libre
SSCC125	-----	10.239.68.125	255.255.255.0	-----	5	SI
SSCC126	-----	10.239.68.126	255.255.255.0	-----	5	SI
SSCC127	-----	10.239.68.127	255.255.255.0	-----	5	SI
SSCC128	-----	10.239.68.128	255.255.255.0	-----	5	SI
SSCC129	-----	10.239.68.129	255.255.255.0	-----	5	SI
SSCC130	-----	10.239.68.130	255.255.255.0	-----	5	SI
SSCC131	-----	10.239.68.131	255.255.255.0	-----	5	SI
SSCC132	-----	10.239.68.132	255.255.255.0	-----	5	SI
SSCC133	-----	10.239.68.133	255.255.255.0	-----	5	SI
SSCC134	-----	10.239.68.134	255.255.255.0	-----	5	SI
SSCC135	-----	10.239.68.135	255.255.255.0	-----	5	SI
SSCC136	-----	10.239.68.136	255.255.255.0	-----	5	SI
SSCC137	-----	10.239.68.137	255.255.255.0	-----	5	SI
SSCC138	-----	10.239.68.138	255.255.255.0	-----	5	SI
SSCC139	-----	10.239.68.139	255.255.255.0	-----	5	SI
SSCC140	Windows 2000	10.239.69.140	255.255.255.0	Dinámica	6	No
SSCC141	Windows 2000	10.239.69.141	255.255.255.0	Dinámica	6	No
SSCC142	Windows 2000	10.239.69.142	255.255.255.0	Dinámica	6	No
SSCC143	Windows 2000	10.239.69.143	255.255.255.0	Dinámica	6	No
SSCC144	Windows 2000	10.239.69.144	255.255.255.0	Dinámica	6	No
SSCC145	Windows 2000	10.239.69.145	255.255.255.0	Dinámica	6	No
SSCC146	Windows 2000	10.239.69.146	255.255.255.0	Dinámica	6	No
SSCC147	Windows 2000	10.239.69.147	255.255.255.0	Dinámica	6	No
SSCC148	Windows 2000	10.239.69.148	255.255.255.0	Dinámica	6	No
SSCC149	Windows 2000	10.239.69.149	255.255.255.0	Dinámica	6	No
SSCC150	Windows 2000	10.239.69.150	255.255.255.0	Dinámica	6	No
SSCC151	Windows XP	10.239.69.151	255.255.255.0	Dinámica	6	No
SSCC152	Windows 2000	10.239.69.152	255.255.255.0	Dinámica	6	No
SSCC153	Windows 2000	10.239.69.153	255.255.255.0	Dinámica	6	No
SSCC154	Windows 2000	10.239.69.154	255.255.255.0	Dinámica	6	No
SSCC155	Windows XP	10.239.69.155	255.255.255.0	Dinámica	6	No

Nombre del dispositivo	Sistema operativo	IP	Mascara Subred	Estatica/ Dinamica	VLAN	Libre
SSCC156	Windows XP	10.239.69.156	255.255.255.0	Dinámica	6	No
SSCC157	Windows 2000	10.239.69.157	255.255.255.0	Dinámica	6	No
SSCC158	Windows 2000	10.239.69.158	255.255.255.0	Dinámica	6	No
SSCC159	Windows 2000	10.239.69.159	255.255.255.0	Dinámica	6	No
SSCC160	Windows 2000	10.239.69.160	255.255.255.0	Dinámica	6	No
SSCC161	Windows 2000	10.239.69.161	255.255.255.0	Dinámica	6	No
SSCC162	Windows 2000	10.239.69.162	255.255.255.0	Dinámica	6	No
SSCC163	Windows 2000	10.239.69.163	255.255.255.0	Dinámica	6	No
SSCC164	Windows XP	10.239.69.164	255.255.255.0	Dinámica	6	No
SSCC165	Windows XP	10.239.69.165	255.255.255.0	Dinámica	6	No
SSCC166	Windows XP	10.239.69.166	255.255.255.0	Dinámica	6	No
SSCC167	Windows XP	10.239.69.167	255.255.255.0	Dinámica	6	No
SSCC168	Windows XP	10.239.69.168	255.255.255.0	Dinámica	6	No
SSCC169	Windows XP	10.239.69.169	255.255.255.0	Dinámica	6	No
SSCC170	Windows XP	10.239.69.170	255.255.255.0	Dinámica	6	No
SSCC171	Windows XP	10.239.69.171	255.255.255.0	Dinámica	6	No
SSCC172	Windows XP	10.239.69.172	255.255.255.0	Dinámica	6	No
SSCC173	Windows XP	10.239.69.173	255.255.255.0	Dinámica	6	No
SSCC174	Windows XP	10.239.69.174	255.255.255.0	Dinámica	6	No
SSCC175	Windows XP	10.239.69.175	255.255.255.0	Dinámica	6	No
SSCC176	-----	10.239.69.176	255.255.255.0	-----	6	SI
SSCC177	-----	10.239.69.177	255.255.255.0	-----	6	SI
SSCC178	-----	10.239.69.178	255.255.255.0	-----	6	SI
SSCC179	-----	10.239.69.179	255.255.255.0	-----	6	SI
SSCC180	-----	10.239.69.180	255.255.255.0	-----	6	SI
SSCC181	-----	10.239.69.181	255.255.255.0	-----	6	SI
SSCC182	-----	10.239.69.182	255.255.255.0	-----	6	SI
SSCC183	-----	10.239.69.183	255.255.255.0	-----	6	SI
SSCC184	-----	10.239.69.184	255.255.255.0	-----	6	SI
SSCC185	-----	10.239.69.185	255.255.255.0	-----	6	SI
SSCC186	-----	10.239.69.186	255.255.255.0	-----	6	SI

Nombre del dispositivo	Sistema operativo	IP	Mascara Subred	Estatica/ Dinamica	VLAN	Libre
SSCC187	-----	10.239.69.187	255.255.255.0	-----	6	SI
SSCC188	-----	10.239.69.188	255.255.255.0	-----	6	SI
SSCC189	-----	10.239.69.189	255.255.255.0	-----	6	SI
SSCC190	-----	10.239.69.190	255.255.255.0	-----	6	SI
SSCC191	-----	10.239.69.191	255.255.255.0	-----	6	SI
SSCC192	-----	10.239.69.192	255.255.255.0	-----	6	SI
SSCC193	-----	10.239.69.193	255.255.255.0	-----	6	SI
SSCC194	-----	10.239.69.194	255.255.255.0	-----	6	SI
SSCC195	-----	10.239.69.195	255.255.255.0	-----	6	SI
SSCC196	-----	10.239.69.196	255.255.255.0	-----	6	SI
SSCC197	-----	10.239.69.197	255.255.255.0	-----	6	SI
SSCC198	-----	10.239.69.198	255.255.255.0	-----	6	SI
SSCC199	-----	10.239.69.199	255.255.255.0	-----	6	SI

Tabla C-6 Equipos Usuarios (VLANs 3,5,6)

PatchPanel	Switch	Interfaz	Equipo
D0.1	ScSwitch05	Fa0/1	INF100
D0.2	ScSwitch05	Fa0/2	INF101
D0.3	ScSwitch05	Fa0/3	INF102
D0.4	ScSwitch05	Fa0/4	INF103
D0.5	ScSwitch05	Fa0/5	INF104
D0.6	ScSwitch05	Fa0/6	INF105
D0.7	ScSwitch05	Fa0/7	INF106
D0.8	ScSwitch05	Fa0/8	INF107
D0.9	ScSwitch05	Fa0/9	INF108
D0.10	ScSwitch05	Fa0/10	INF109
D0.11	ScSwitch05	Fa0/11	INF110
D0.12	ScSwitch05	Fa0/12	INF111
D0.13	ScSwitch05	Fa0/13	INF112
D0.14	ScSwitch05	Fa0/14	INF113
D0.15	ScSwitch05	Fa0/15	INF114
D0.16	ScSwitch05	Fa0/16	INF115
D0.17	ScSwitch05	Fa0/17	INF116
D0.18	ScSwitch05	Fa0/18	PRUEBAS
D0.19	ScSwitch05	Fa0/19	IMPRESORA65200
D0.20	ScSwitch05	Fa0/20	IMPRESORA65201
D0.21	ScSwitch05	Fa0/21	APAGADA
D0.22	ScSwitch05	Fa0/22	Arpwatch Odonell
D0.23	ScSwitch05	Fa0/23	Arpwatch Olive
D0.24	ScSwitch05	Fa0/24	Arpwatch Bilbao
D0.25	ScSwitch06	Fa0/1	APAGADA
D0.26	ScSwitch06	Fa0/2	APAGADA
D0.27	ScSwitch06	Fa0/3	APAGADA
D0.28	ScSwitch06	Fa0/4	APAGADA
D0.29	ScSwitch06	Fa0/5	APAGADA
D0.30	ScSwitch06	Fa0/6	APAGADA
D0.31	ScSwitch06	Fa0/7	APAGADA

PatchPanel	Switch	Interfaz	Equipo
D0.32	ScSwitch06	Fa0/8	APAGADA
D0.33	ScSwitch06	Fa0/9	SSCC040
D0.34	ScSwitch06	Fa0/10	SSCC041
D0.35	ScSwitch06	Fa0/11	SSCC042
D0.36	ScSwitch06	Fa0/12	SSCC043
D0.37	ScSwitch06	Fa0/13	SSCC044
D0.38	ScSwitch06	Fa0/14	SSCC045
D0.39	ScSwitch06	Fa0/15	SSCC046
D0.40	ScSwitch06	Fa0/16	SSCC047
D0.41	ScSwitch06	Fa0/17	SSCC048
D0.42	ScSwitch06	Fa0/18	SSCC049
D0.43	ScSwitch06	Fa0/19	IMPRESORA66206
D0.44	ScSwitch06	Fa0/20	IMPRESORA66207
D0.45	ScSwitch06	Fa0/21	APAGADA
D0.46	ScSwitch06	Fa0/22	APAGADA
D0.47	ScSwitch06	Fa0/23	APAGADA
D0.48 - AntenaBi	ScSwitch06	Fa0/24	PuenteSsccBilbao
D0.49	ScSwitch07	Fa0/1	APAGADA
D0.50	ScSwitch07	Fa0/2	APAGADA
D0.51	ScSwitch07	Fa0/3	APAGADA
D0.52	ScSwitch07	Fa0/4	SSCC004
D0.53	ScSwitch07	Fa0/5	SSCC005
D0.54	ScSwitch07	Fa0/6	SSCC006
D0.55	ScSwitch07	Fa0/7	SSCC007
D0.56	ScSwitch07	Fa0/8	SSCC008
D0.57	ScSwitch07	Fa0/9	SSCC009
D0.58	ScSwitch07	Fa0/10	SSCC010
D0.59	ScSwitch07	Fa0/11	SSCC011
D0.60	ScSwitch07	Fa0/12	SSCC012
D0.61	ScSwitch07	Fa0/13	SSCC013
D0.62	ScSwitch07	Fa0/14	SSCC014

PatchPanel	Switch	Interfaz	Equipo
D0.63	ScSwitch07	Fa0/15	IMPRESORA66208
D0.64	ScSwitch07	Fa0/16	APAGADA
D0.65	ScSwitch07	Fa0/17	APAGADA
D0.66	ScSwitch07	Fa0/18	APAGADA
D0.67	ScSwitch07	Fa0/19	APAGADA
D0.68	ScSwitch07	Fa0/20	APAGADA
D0.69	ScSwitch07	Fa0/21	APAGADA
D0.70	ScSwitch07	Fa0/22	APAGADA
D0.71	ScSwitch07	Fa0/23	APAGADA
D0.72 - AntenaOd	ScSwitch07	Fa0/24	PuenteSsccOdonell
AntenaBiBackup	-----	-----	-----
AntenaOdBackup	-----	-----	-----

Tabla C-7 CPD

PatchPanel	Switch	Interfaz	Equipo
D1	Switch11	Fa0/1	SSCC059
D2	Switch11	Fa0/2	SSCC058
D3	Switch11	Fa0/3	SSCC057
D4	Switch11	Fa0/4	APAGADA
D5	Switch11	Fa0/5	APAGADA
D6	Switch11	Fa0/6	APAGADA
D7	Switch11	Fa0/7	APAGADA
D8	Switch11	Fa0/8	APAGADA
D9	Switch11	Fa0/9	APAGADA
D10	Switch11	Fa0/10	APAGADA
D11	Switch11	Fa0/11	APAGADA
D12	Switch11	Fa0/12	APAGADA
D13	Switch11	Fa0/13	APAGADA
D14	Switch11	Fa0/14	SSCC050
D15	Switch11	Fa0/15	SSCC051
D16	Switch11	Fa0/16	IMPRESORA66200
D17	Switch11	Fa0/17	SSCC052
D18	Switch11	Fa0/18	SSCC053
D19	Switch11	Fa0/19	SSCC054
D20	Switch11	Fa0/20	APAGADA
D21	Switch11	Fa0/21	APAGADA
D22	Switch11	Fa0/22	APAGADA
D23	Switch11	Fa0/23	APAGADA
D24	Switch11	Fa0/24	APAGADA
D25	Switch12	Fa0/1	SSCC055
D26	Switch12	Fa0/2	SSCC056
D27	Switch12	Fa0/3	SSCC060
D28	Switch12	Fa0/4	SSCC061
D29	Switch12	Fa0/5	SSCC062
D30	Switch12	Fa0/6	IMPRESORA66201
D31	Switch12	Fa0/7	IMPRESORA66202

PatchPanel	Switch	Interfaz	Equipo
D32	Switch12	Fa0/8	IMPRESORA66203
D33	Switch12	Fa0/9	IMPRESORA66204
D34	Switch12	Fa0/10	APAGADA
D35	Switch12	Fa0/11	APAGADA
D36	Switch12	Fa0/12	APAGADA
D37	Switch12	Fa0/13	APAGADA
D38	Switch12	Fa0/14	APAGADA
D39	Switch12	Fa0/15	SSCC030
D40	Switch12	Fa0/16	SSCC031
D41	Switch12	Fa0/17	SSCC032
D42	Switch12	Fa0/18	SSCC033
D43	Switch12	Fa0/19	SSCC034
D44	Switch12	Fa0/20	SSCC035
D45	Switch12	Fa0/21	SSCC036
D46	Switch12	Fa0/22	SSCC037
D47	Switch12	Fa0/23	SSCC038
D48	Switch12	Fa0/24	SSCC039
D49	Switch13	Fa0/1	APAGADA
D50	Switch13	Fa0/2	APAGADA
D51	Switch13	Fa0/3	APAGADA
D52	Switch13	Fa0/4	APAGADA
D53	Switch13	Fa0/5	APAGADA
D54	Switch13	Fa0/6	APAGADA
D55	Switch13	Fa0/7	SSCC020
D56	Switch13	Fa0/8	SSCC021
D57	Switch13	Fa0/9	SSCC022
D58	Switch13	Fa0/10	SSCC023
D59	Switch13	Fa0/11	SSCC024
D60	Switch13	Fa0/12	SSCC025
D61	Switch13	Fa0/13	SSCC026
D62	Switch13	Fa0/14	SSCC027

PatchPanel	Switch	Interfaz	Equipo
D63	Switch13	Fa0/15	SSCC028
D64	Switch13	Fa0/16	SSCC029
D65	Switch13	Fa0/17	IMPRESORA205
D66	Switch13	Fa0/18	APAGADA
D67	Switch13	Fa0/19	APAGADA
D68	Switch13	Fa0/20	APAGADA
D69	Switch13	Fa0/21	APAGADA
D70	Switch13	Fa0/22	APAGADA
D71	Switch13	Fa0/23	APAGADA
D72	Switch13	Fa0/24	APAGADA
D73	Switch14	Fa0/1	APAGADA
D74	Switch14	Fa0/2	APAGADA
D75	Switch14	Fa0/3	APAGADA
D76	Switch14	Fa0/4	APAGADA
D77	Switch14	Fa0/5	APAGADA
D78	Switch14	Fa0/6	APAGADA
D79	Switch14	Fa0/7	APAGADA
D80	Switch14	Fa0/8	APAGADA
D81	Switch14	Fa0/9	APAGADA
D82	Switch14	Fa0/10	SSCC015
D83	Switch14	Fa0/11	SSCC016
D84	Switch14	Fa0/12	APAGADA
D85	Switch14	Fa0/13	SSCC017
D86	Switch14	Fa0/14	APAGADA
D87	Switch14	Fa0/15	APAGADA
D88	Switch14	Fa0/16	SSCC018
D89	Switch14	Fa0/17	SSCC019
D90	Switch14	Fa0/18	APAGADA
D91	Switch14	Fa0/19	APAGADA
D92	Switch14	Fa0/20	APAGADA
D93	Switch14	Fa0/21	APAGADA

PatchPanel	Switch	Interfaz	Equipo
D94	Switch14	Fa0/22	APAGADA
D95	Switch14	Fa0/23	APAGADA
D96	Switch14	Fa0/24	SAI4
D97	Sin asignar	-----	-----
D98	Sin asignar	-----	-----
D99	Sin asignar	-----	-----
D100	Sin asignar	-----	-----
D101	Sin asignar	-----	-----
D102	Sin asignar	-----	-----
D103	Sin asignar	-----	-----
D104	Sin asignar	-----	-----
D105	Sin asignar	-----	-----
D106	Sin asignar	-----	-----
D107	Sin asignar	-----	-----
D108	Sin asignar	-----	-----
D109	Sin asignar	-----	-----
D110	Sin asignar	-----	-----
D111	Sin asignar	-----	-----
D112	Sin asignar	-----	-----
D113	Sin asignar	-----	-----
D114	Sin asignar	-----	-----
D115	Sin asignar	-----	-----
D116	Sin asignar	-----	-----

Tabla C-8 Pasillo

PatchPanel	Switch	Interfaz	Equipo
0.01	BiSwitch01	Fa0/1	SSCC070
0.02	BiSwitch01	Fa0/2	SSCC071
0.03	BiSwitch01	Fa0/3	SSCC072
0.04	BiSwitch01	Fa0/4	SSCC073
0.05	BiSwitch01	Fa0/5	IMPRESORA68200
0.06	BiSwitch01	Fa0/6	SSCC074
0.07	BiSwitch01	Fa0/7	SSCC075
0.08	BiSwitch01	Fa0/8	SSCC076
0.09	BiSwitch01	Fa0/9	IMPRESORA68201
0.10	BiSwitch01	Fa0/10	SSCC077
0.11	BiSwitch01	Fa0/11	SSCC078
0.12	BiSwitch01	Fa0/12	SSCC079
0.13	BiSwitch01	Fa0/13	SSCC080
0.14	BiSwitch01	Fa0/14	SSCC081
1.01	BiSwitch01	Fa0/15	SSCC082
1.02	BiSwitch01	Fa0/16	SSCC083
1.03	BiSwitch01	Fa0/17	SSCC084
1.04	BiSwitch01	Fa0/18	SSCC085
1.05	BiSwitch01	Fa0/19	IMPRESORA68202
1.06	BiSwitch01	Fa0/20	IMPRESORA68203
1.07	BiSwitch01	Fa0/21	IMPRESORA68204
1.08	BiSwitch01	Fa0/22	SSCC124
1.09	BiSwitch01	Fa0/23	APAGADA
1.10 - Antena	BiSwitch01	Fa0/24	PuenteBilbao
1.11	BiSwitch02	Fa0/1	SSCC086
1.12	BiSwitch02	Fa0/2	SSCC087
1.13	BiSwitch02	Fa0/3	SSCC088
1.14	BiSwitch02	Fa0/4	SSCC089
1.15	BiSwitch02	Fa0/5	SSCC090
1.16	BiSwitch02	Fa0/6	SSCC091
1.17	BiSwitch02	Fa0/7	SSCC092

PatchPanel	Switch	Interfaz	Equipo
1.18	BiSwitch02	Fa0/8	SSCC093
1.19	BiSwitch02	Fa0/9	SSCC094
1.20	BiSwitch02	Fa0/10	SSCC095
1.21	BiSwitch02	Fa0/11	SSCC096
1.22	BiSwitch02	Fa0/12	SSCC097
2.01	BiSwitch02	Fa0/13	SSCC098
2.02	BiSwitch02	Fa0/14	SSCC099
2.03	BiSwitch02	Fa0/15	SSCC100
2.04	BiSwitch02	Fa0/16	SSCC101
2.05	BiSwitch02	Fa0/17	IMPRESORA68205
2.06	BiSwitch02	Fa0/18	IMPRESORA68206
2.07	BiSwitch02	Fa0/19	IMPRESORA68207
2.08	BiSwitch02	Fa0/20	SSCC101
2.09	BiSwitch02	Fa0/21	SSCC102
2.10	BiSwitch02	Fa0/22	SSCC103
2.11	BiSwitch02	Fa0/23	SSCC104
2.12	BiSwitch02	Fa0/24	SSCC105
2.13	BiSwitch03	Fa0/1	SSCC106
2.14	BiSwitch03	Fa0/2	SSCC107
2.15	BiSwitch03	Fa0/3	SSCC108
2.16	BiSwitch03	Fa0/4	SSCC109
2.17	BiSwitch03	Fa0/5	SSCC110
2.18	BiSwitch03	Fa0/6	SSCC111
2.19	BiSwitch03	Fa0/7	SSCC112
2.20	BiSwitch03	Fa0/8	SSCC113
2.21	BiSwitch03	Fa0/9	SSCC114
2.22	BiSwitch03	Fa0/10	SSCC115
2.23	BiSwitch03	Fa0/11	SSCC116
2.24	BiSwitch03	Fa0/12	SSCC117
3.03	BiSwitch03	Fa0/13	SSCC117
3.04	BiSwitch03	Fa0/14	SSCC118

PatchPanel	Switch	Interfaz	Equipo
3.05	BiSwitch03	Fa0/15	IMPRESORA68208
3.06	BiSwitch03	Fa0/16	SSCC119
3.08	BiSwitch03	Fa0/17	SSCC120
3.07	BiSwitch03	Fa0/18	SSCC121
3.08	BiSwitch03	Fa0/19	SSCC122
3.09	BiSwitch03	Fa0/20	SSCC123
3.10	BiSwitch03	Fa0/21	IMPRESORA68209
3.11	BiSwitch03	Fa0/22	BiSAI1
3.12	BiSwitch03	Fa0/23	APAGADA
3.13	BiSwitch03	Fa0/24	APAGADA
AntenaBackup	-----	-----	-----

Tabla C-9 Bilbao

PatchPanel	Switch	Interfaz	Equipo
D1	OdSwitch41	**Fa0/1**	SSCC140
D2	OdSwitch41	**Fa0/2**	SSCC141
D3	OdSwitch41	**Fa0/3**	SSCC142
D4	OdSwitch41	**Fa0/4**	SSCC143
D5	OdSwitch41	**Fa0/5**	SSCC144
D6	OdSwitch41	**Fa0/6**	SSCC145
D7	OdSwitch41	**Fa0/7**	IMPRESORA69204
D8	OdSwitch41	**Fa0/8**	APAGADO
D9	OdSwitch41	**Fa0/9**	APAGADO
D10	OdSwitch41	**Fa0/10**	IMPRESORA69200
D11	OdSwitch41	**Fa0/11**	IMPRESORA69201
D12	OdSwitch41	**Fa0/12**	SSCC146
D13	OdSwitch41	**Fa0/13**	SSCC147
D14	OdSwitch41	**Fa0/14**	SSCC148
D15	OdSwitch41	**Fa0/15**	SSCC149
D16	OdSwitch41	**Fa0/16**	SSCC150
D17	OdSwitch41	**Fa0/17**	SSCC151
D18	OdSwitch41	**Fa0/18**	SSCC152
D19	OdSwitch41	**Fa0/19**	SSCC153
D20	OdSwitch41	**Fa0/20**	SSCC154
D21	OdSwitch41	**Fa0/21**	SSCC155
D22	OdSwitch41	**Fa0/22**	SSCC156
D23	OdSwitch41	**Fa0/23**	OdSAI1
Antena	OdSwitch41	**Fa0/24**	PuenteOdonell
D24	OdSwitch42	**Fa0/1**	SSCC157
D25	OdSwitch42	**Fa0/2**	SSCC158
D26	OdSwitch42	**Fa0/3**	IMPRESORA69202
D27	OdSwitch42	**Fa0/4**	SSCC159
D28	OdSwitch42	**Fa0/5**	SSCC160
D29	OdSwitch42	**Fa0/6**	SSCC161
D29	OdSwitch42	**Fa0/7**	SSCC162
D30	OdSwitch42	**Fa0/8**	APAGADO
D31	OdSwitch42	**Fa0/9**	IMPRESORA69203
D32	OdSwitch42	**Fa0/10**	SSCC163

PatchPanel	Switch	Interfaz	Equipo
D33	OdSwitch42	**Fa0/11**	SSCC164
D34	OdSwitch42	**Fa0/12**	SSCC165
D35	OdSwitch42	**Fa0/13**	SSCC166
D36	OdSwitch42	**Fa0/14**	SSCC167
D37	OdSwitch42	**Fa0/15**	SSCC168
D38	OdSwitch42	**Fa0/16**	SSCC169
D39	OdSwitch42	**Fa0/17**	SSCC170
D40	OdSwitch42	**Fa0/18**	SSCC171
D41	OdSwitch42	**Fa0/19**	SSCC172
D42	OdSwitch42	**Fa0/20**	SSCC173
D43	OdSwitch42	**Fa0/21**	SSCC174
D44	OdSwitch42	**Fa0/22**	SSCC175
D45	OdSwitch42	**Fa0/23**	APAGADO
D46	OdSwitch42	**Fa0/24**	APAGADO
D47	-----	-----	-----
D48	-----	-----	-----
D49	-----	-----	-----
D50	-----	-----	-----
D51	-----	-----	-----
D52	-----	-----	-----
D53	-----	-----	-----
D54	-----	-----	-----
D55	-----	-----	-----
D56	-----	-----	-----
D57	-----	-----	-----
D58	-----	-----	-----
D59	-----	-----	-----
D60	-----	-----	-----
AntenaBakup	-----	-----	-----

Tabla C-10 O'Donell

Catalyst 2960 10.239.64.10	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN
ScSwitch02	Gi0/1	Hades(WebServer)	1000	FULL	FWD	SI	NO	NO	99
ScSwitch02	Gi0/2	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/3	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/4	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/5	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/6	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/7	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/8	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/9	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/10	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/11	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/12	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/13	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/14	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/15	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/16	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/17	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/18	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/19	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/20	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/21	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/22	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/23	Firewall(Cervero1)	1000	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/24	Firewall(Cervero2)	1000	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/25	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/26	-----	-----	-----	-----	-----	-----	-----	-----

Tabla C-11 DMZ

Catalyst 3560 10.239.71.2	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN
ScSwitch01	Gi0/1	Po1-ScSwitch02	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch01	Gi0/2	Po1-ScSwitch02	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch01	Gi0/3	Po2-ScSwitch03	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch01	Gi0/4	Po2-ScSwitch03	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch01	Gi0/5	Po4-ScSwitch04	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch01	Gi0/6	Po4-ScSwitch04	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch01	Gi0/7	Conecta Gi0/1 ScSwitch05	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch01	Gi0/8	Conecta Gi0/1 ScSwitch06	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch01	Gi0/9	Conecta Gi0/1 ScSwitch07	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch01	Gi0/10	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch01	Gi0/11	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch01	Gi0/12	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch01	Gi0/13	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch01	Gi0/14	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch01	Gi0/15	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch01	Gi0/16	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch01	Gi0/17	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch01	Gi0/18	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch01	Gi0/19	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch01	Gi0/20	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch01	Gi0/21	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch01	Gi0/22	Monitor	1000	FULL	FWD	NO	NO	NO	-----
ScSwitch01	Gi0/23	RCJA	1000	FULL	FWD	NO	NO	NO	ENRUTADA
ScSwitch01	Gi0/24	Conecta Gi0/1 ScSwitch14	1000	FULL	FWD	NO	SI	NO	TRUNK
ScSwitch01	Gi0/25	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch01	Gi0/26	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch01	Gi0/27	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch01	Gi0/28	-----	-----	-----	-----	-----	-----	-----	-----

Tabla C-12 ScSwitch01

Catalyst 3560 10.239.71.3	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN
ScSwitch02	Gi0/1	Po1-ScSwitch01	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/2	Po1-ScSwitch01	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/3	Po3-ScSwitch03	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/4	Po3-ScSwitch03	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/5	Po5-ScSwitch04	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/6	Po5-ScSwitch04	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/7	Conecta Gi0/2 ScSwitch05	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/8	Conecta Gi0/2 ScSwitch07	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/9	Conecta Gi0/2 ScSwitch06	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/10	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/11	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/12	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/13	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/14	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/15	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/16	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/17	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/18	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/19	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/20	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/21	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/22	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/23	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/24	RCJA	1000	FULL	FWD	NO	NO	NO	ENRUTADA
ScSwitch02	Gi0/25	Conecta Gi0/1 ScSwitch11	1000	FULL	FWD	NO	SI	NO	TRUNK
ScSwitch02	Gi0/26	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/27	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/28	-----	-----	-----	-----	-----	-----	-----	-----

Tabla C-13 ScSwitch02

Catalyst 2960 10.239.71.103	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN
ScSwitch02	Gi0/1	Po2-ScSwitch01	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/2	Po2-ScSwitch01	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/3	Po3-ScSwitch02	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/4	Po3-ScSwitch02	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/5	Neptuno(DBServer1)	1000	FULL	FWD	Si	NO	NO	4
ScSwitch02	Gi0/6	Hefesto(Webinterno)	1000	FULL	FWD	Si	NO	NO	4
ScSwitch02	Gi0/7	Poseidon(DBServer2)	1000	FULL	FWD	Si	NO	NO	4
ScSwitch02	Gi0/8	Atenea1(Proxy)	1000	FULL	FWD	Si	NO	NO	4
ScSwitch02	Gi0/9	Atenea2(Dns)	1000	FULL	FWD	Si	NO	NO	4
ScSwitch02	Gi0/10	Afrodita(Dominio1)	1000	FULL	FWD	Si	NO	NO	4
ScSwitch02	Gi0/11	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/12	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/13	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/14	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/15	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/16	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/17	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/18	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/19	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/20	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/21	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/22	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/23	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/24	-----	-----	-----	-----	-----	-----	-----	-----

Tabla C-14 ScSwitch03

Catalyst 2960 10.239.71.104	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN
ScSwitch02	Gi0/1	Po2-ScSwitch01	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/2	Po2-ScSwitch01	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/3	Po3-ScSwitch02	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/4	Po3-ScSwitch02	1000	FULL	FWD	NO	SI	SI	TRUNK
ScSwitch02	Gi0/5	Helios(Monitorizacion)	1000	FULL	FWD	Si	NO	NO	4
ScSwitch02	Gi0/6	Apolo(Servidor Impresion)	1000	FULL	FWD	Si	NO	NO	4
ScSwitch02	Gi0/7	Backup	1000	FULL	FWD	Si	NO	NO	4
ScSwitch02	Gi0/8	Desarrollo1	1000	FULL	FWD	Si	NO	NO	4
ScSwitch02	Gi0/9	Desarrollo2	1000	FULL	FWD	Si	NO	NO	4
ScSwitch02	Gi0/10	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/11	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/12	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/13	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/14	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/15	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/16	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/17	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/18	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/19	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/20	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/21	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/22	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/23	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/24	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/25	-----	-----	-----	-----	-----	-----	-----	-----
ScSwitch02	Gi0/26	-----	-----	-----	-----	-----	-----	-----	-----

Tabla C-15 ScSwitch04

Catalyst 2960 10.239.71.105	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN	Información de la localización
ScSwitch05	Fa0/1	INF100	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.1
ScSwitch05	Fa0/2	INF101	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.2
ScSwitch05	Fa0/3	INF102	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.3
ScSwitch05	Fa0/4	INF103	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.4
ScSwitch05	Fa0/5	INF104	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.5
ScSwitch05	Fa0/6	INF105	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.6
ScSwitch05	Fa0/7	INF106	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.7
ScSwitch05	Fa0/8	INF107	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.8
ScSwitch05	Fa0/9	INF108	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.9
ScSwitch05	Fa0/10	INF109	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.10
ScSwitch05	Fa0/11	INF110	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.11
ScSwitch05	Fa0/12	INF111	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.12
ScSwitch05	Fa0/13	INF112	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.13
ScSwitch05	Fa0/14	INF113	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.14
ScSwitch05	Fa0/15	INF114	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.15
ScSwitch05	Fa0/16	INF115	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.16
ScSwitch05	Fa0/17	INF116	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.17
ScSwitch05	Fa0/18	PRUEBAS	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.18
ScSwitch05	Fa0/19	IMPRESORA65200	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.19
ScSwitch05	Fa0/20	IMPRESORA65201	100	FULL	FWD	Si	NO	NO	2	Patch Panel del CPD D0.20
ScSwitch05	Fa0/21	APAGADA	-----	-----	-----	-----	-----	-----	2	Patch Panel del CPD D0.21
ScSwitch05	Fa0/22	Arpwatch Odonell	100	FULL	FWD	Si	NO	NO	6	Patch Panel del CPD D0.22
ScSwitch05	Fa0/23	Arpwatch Olive	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.23
ScSwitch05	Fa0/24	Arpwatch Bilbao	100	FULL	FWD	Si	NO	NO	5	Patch Panel del CPD D0.24
ScSwitch05	Gi0/1	Conectada ScSwitch01	1000	FULL	FWD	NO	Si	NO	TRUNK	-----
ScSwitch05	Gi0/2	Conectada ScSwitch02	1000	FULL	BLK	NO	Si	NO	TRUNK	-----

Tabla C-16 ScSwitch05

Catalyst 2960 10.239.71.106	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN	Información de la localización
ScSwitch06	Fa0/1	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.25
ScSwitch06	Fa0/2	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.26
ScSwitch06	Fa0/3	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.27
ScSwitch06	Fa0/4	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.28
ScSwitch06	Fa0/5	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.29
ScSwitch06	Fa0/6	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.30
ScSwitch06	Fa0/7	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.31
ScSwitch06	Fa0/8	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.32
ScSwitch06	Fa0/9	SSCC040	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.33
ScSwitch06	Fa0/10	SSCC041	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.34
ScSwitch06	Fa0/11	SSCC042	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.35
ScSwitch06	Fa0/12	SSCC043	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.36
ScSwitch06	Fa0/13	SSCC044	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.37
ScSwitch06	Fa0/14	SSCC045	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.38
ScSwitch06	Fa0/15	SSCC046	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.39
ScSwitch06	Fa0/16	SSCC047	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.40
ScSwitch06	Fa0/17	SSCC048	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.41
ScSwitch06	Fa0/18	SSCC049	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.42
ScSwitch06	Fa0/19	IMPRESORA66206	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.43
ScSwitch06	Fa0/20	IMPRESORA66207	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.44
ScSwitch06	Fa0/21	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.45
ScSwitch06	Fa0/22	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.46
ScSwitch06	Fa0/23	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.47
ScSwitch06	Fa0/24	PuenteSsccBilbao	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.48 - AntenaBi
ScSwitch06	Gi0/1	Conectada ScSwitch01	1000	FULL	FWD	NO	Si	NO	TRUNK	-----
ScSwitch06	Gi0/2	Conectada ScSwitch02	1000	FULL	BLK	NO	Si	NO	TRUNK	-----

Tabla C-17 ScSwitch06

Catalyst 2960 10.239.71.107	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN	Información de la localización
ScSwitch07	Fa0/1	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.49
ScSwitch07	Fa0/2	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.50
ScSwitch07	Fa0/3	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.51
ScSwitch07	Fa0/4	SSCC004	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.52
ScSwitch07	Fa0/5	SSCC005	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.53
ScSwitch07	Fa0/6	SSCC006	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.54
ScSwitch07	Fa0/7	SSCC007	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.55
ScSwitch07	Fa0/8	SSCC008	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.56
ScSwitch07	Fa0/9	SSCC009	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.57
ScSwitch07	Fa0/10	SSCC010	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.58
ScSwitch07	Fa0/11	SSCC011	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.59
ScSwitch07	Fa0/12	SSCC012	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.60
ScSwitch07	Fa0/13	SSCC013	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.61
ScSwitch07	Fa0/14	SSCC014	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.62
ScSwitch07	Fa0/15	IMPRESORA66208	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.63
ScSwitch07	Fa0/16	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.64
ScSwitch07	Fa0/17	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.65
ScSwitch07	Fa0/18	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.66
ScSwitch07	Fa0/19	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.67
ScSwitch07	Fa0/20	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.68
ScSwitch07	Fa0/21	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.69
ScSwitch07	Fa0/22	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.70
ScSwitch07	Fa0/23	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del CPD D0.71
ScSwitch07	Fa0/24	PuenteSsccOdonell	100	FULL	FWD	Si	NO	NO	3	Patch Panel del CPD D0.72 - AntenaOd
ScSwitch07	Gi0/1	Conectada ScSwitch01	1000	FULL	FWD	NO	Si	NO	TRUNK	-----
ScSwitch07	Gi0/2	Conectada ScSwitch02	1000	FULL	BLK	NO	Si	NO	TRUNK	-----

Tabla C-18 ScSwitch07

Catalyst 2960 10.239.71.111	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN	Información de la localización
Switch11	Fa0/1	SSCC059	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D1
Switch11	Fa0/2	SSCC058	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D2
Switch11	Fa0/3	SSCC057	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D3
Switch11	Fa0/4	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D4
Switch11	Fa0/5	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D5
Switch11	Fa0/6	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D6
Switch11	Fa0/7	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D7
Switch11	Fa0/8	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D8
Switch11	Fa0/9	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D9
Switch11	Fa0/10	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D10
Switch11	Fa0/11	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D11
Switch11	Fa0/12	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D12
Switch11	Fa0/13	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D13
Switch11	Fa0/14	SSCC050	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D14
Switch11	Fa0/15	SSCC051	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D15
Switch11	Fa0/16	IMPRESORA66200	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D16
Switch11	Fa0/17	SSCC052	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D17
Switch11	Fa0/18	SSCC053	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D18
Switch11	Fa0/19	SSCC054	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D19
Switch11	Fa0/20	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D20
Switch11	Fa0/21	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D21
Switch11	Fa0/22	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D22
Switch11	Fa0/23	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D23
Switch11	Fa0/24	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D24
Switch11	Gi0/1	Conectado a ScSwitch02	1000	FULL	BLK	NO	Si	NO	TRUNK	-----
Switch11	Gi0/2	Conectado a ScSwitch12	1000	FULL	BLK	NO	Si	NO	TRUNK	-----
Switch11	Gi0/3	Conectado a ScSwitch14	1000	FULL	FWD	NO	Si	NO	TRUNK	-----
Switch11	Gi0/4	APAGADA	-----	-----	-----	-----	-----	-----	-----	-----

Tabla C-19 ScSwitch11

Catalyst 2960 10.239.71.112	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN	Información de la localización
Switch12	Fa0/1	SSCC055	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D25
Switch12	Fa0/2	SSCC056	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D26
Switch12	Fa0/3	SSCC060	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D27
Switch12	Fa0/4	SSCC061	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D28
Switch12	Fa0/5	SSCC062	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D29
Switch12	Fa0/6	IMPRESORA66201	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D30
Switch12	Fa0/7	IMPRESORA66202	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D31
Switch12	Fa0/8	IMPRESORA66203	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D32
Switch12	Fa0/9	IMPRESORA66204	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D33
Switch12	Fa0/10	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D34
Switch12	Fa0/11	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D35
Switch12	Fa0/12	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D36
Switch12	Fa0/13	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D37
Switch12	Fa0/14	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D38
Switch12	Fa0/15	SSCC030	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D39
Switch12	Fa0/16	SSCC031	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D40
Switch12	Fa0/17	SSCC032	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D41
Switch12	Fa0/18	SSCC033	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D42
Switch12	Fa0/19	SSCC034	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D43
Switch12	Fa0/20	SSCC035	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D44
Switch12	Fa0/21	SSCC036	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D45
Switch12	Fa0/22	SSCC037	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D46
Switch12	Fa0/23	SSCC038	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D47
Switch12	Fa0/24	SSCC039	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D48
Switch12	Gi0/1	Conectado Switch11	1000	FULL	FWD	NO	Si	NO	TRUNK	-----
Switch12	Gi0/2	Conectado Switch13	1000	FULL	FWD	NO	Si	NO	TRUNK	-----

Tabla C-20 ScSwitch12

Catalyst 2960 10,239,71,113	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN	Información de la localización
Switch13	Fa0/1	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D49
Switch13	Fa0/2	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D50
Switch13	Fa0/3	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D51
Switch13	Fa0/4	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D52
Switch13	Fa0/5	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D53
Switch13	Fa0/6	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D54
Switch13	Fa0/7	SSCC020	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D55
Switch13	Fa0/8	SSCC021	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D56
Switch13	Fa0/9	SSCC022	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D57
Switch13	Fa0/10	SSCC023	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D58
Switch13	Fa0/11	SSCC024	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D59
Switch13	Fa0/12	SSCC025	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D60
Switch13	Fa0/13	SSCC026	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D61
Switch13	Fa0/14	SSCC027	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D62
Switch13	Fa0/15	SSCC028	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D63
Switch13	Fa0/16	SSCC029	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D64
Switch13	Fa0/17	IMPRESORA205	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D65
Switch13	Fa0/18	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D66
Switch13	Fa0/19	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D67
Switch13	Fa0/20	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D68
Switch13	Fa0/21	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D69
Switch13	Fa0/22	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D70
Switch13	Fa0/23	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D71
Switch13	Fa0/24	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D72
Switch13	Gi0/1	Conectada Switch12	1000	FULL	FWD	NO	Si	NO	TRUNK	-----
Switch13	Gi0/2	Conectada Switch14	1000	FULL	FWD	NO	Si	NO	TRUNK	-----

Tabla C-21 ScSwitch13

Catalyst 2960 10,239,71,113	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN	Información de la localización
Switch14	Fa0/1	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D73
Switch14	Fa0/2	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D74
Switch14	Fa0/3	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D75
Switch14	Fa0/4	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D76
Switch14	Fa0/5	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D77
Switch14	Fa0/6	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D78
Switch14	Fa0/7	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D79
Switch14	Fa0/8	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D80
Switch14	Fa0/9	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D81
Switch14	Fa0/10	SSCC015	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D82
Switch14	Fa0/11	SSCC016	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D83
Switch14	Fa0/12	SSCC017	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D84
Switch14	Fa0/13	SSCC018	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D85
Switch14	Fa0/14	SSCC019	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D86
Switch14	Fa0/15	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D87
Switch14	Fa0/16	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D88
Switch14	Fa0/17	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D89
Switch14	Fa0/18	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D90
Switch14	Fa0/19	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D91
Switch14	Fa0/20	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D92
Switch14	Fa0/21	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D93
Switch14	Fa0/22	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D94
Switch14	Fa0/23	APAGADA	-----	-----	-----	-----	-----	-----	3	Patch Panel del pasillo D95
Switch14	Fa0/24	SAI4	100	FULL	FWD	Si	NO	NO	3	Patch Panel del pasillo D96
Switch14	Gi0/1	Conectada ScSwitch01	1000	FULL	FWD	NO	Si	NO	TRUNK	-----
Switch14	Gi0/2	Conectada ScSwitch13	1000	FULL	FWD	NO	Si	NO	TRUNK	-----
Switch14	Gi0/3	Conectada ScSwitch11	1000	FULL	FWD	NO	Si	NO	TRUNK	-----
Switch14	Gi0/4	APAGADA	-----	-----	-----	-----	-----	-----	-----	-----

Tabla C-22 ScSwitch14

Catalyst 2960 10.239.68.241	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN	Información de la localización
BiSwitch01	Fa0/1	SSCC070	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 0.01
BiSwitch01	Fa0/2	SSCC071	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 0.02
BiSwitch01	Fa0/3	SSCC072	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 0.03
BiSwitch01	Fa0/4	SSCC073	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 0.04
BiSwitch01	Fa0/5	IMPRESORA68200	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 0.05
BiSwitch01	Fa0/6	SSCC074	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 0.06
BiSwitch01	Fa0/7	SSCC075	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 0.07
BiSwitch01	Fa0/8	SSCC076	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 0.08
BiSwitch01	Fa0/9	IMPRESORA68201	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 0.09
BiSwitch01	Fa0/10	SSCC077	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 0.10
BiSwitch01	Fa0/11	SSCC078	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 0.11
BiSwitch01	Fa0/12	SSCC079	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 0.12
BiSwitch01	Fa0/13	SSCC080	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 0.13
BiSwitch01	Fa0/14	SSCC081	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 0.14
BiSwitch01	Fa0/15	SSCC082	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.01
BiSwitch01	Fa0/16	SSCC083	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.02
BiSwitch01	Fa0/17	SSCC084	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.03
BiSwitch01	Fa0/18	SSCC085	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.04
BiSwitch01	Fa0/19	IMPRESORA68202	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.05
BiSwitch01	Fa0/20	IMPRESORA68203	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.06
BiSwitch01	Fa0/21	IMPRESORA68204	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.07
BiSwitch01	Fa0/22	SSCC124	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.08
BiSwitch01	Fa0/23	APAGADA	-----	-----	-----	-----	-----	-----	5	Patch Panel de Bilbao 1.09
BiSwitch01	Fa0/24	PuenteBilbao	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.10 - Antena
BiSwitch01	Gi0/1	Conectado BiSwitch02	1000	FULL	FWD	NO	Si	NO	Trunk	-----
BiSwitch01	Gi0/2	Conectado BiSwitch03	1000	FULL	FWD	NO	Si	NO	Trunk	-----

Tabla C-23 BiSwitch01

Catalyst 2960 10.239.68.242	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN	Información de la localización
BiSwitch02	Fa0/1	SSCC086	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.11
BiSwitch02	Fa0/2	SSCC087	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.12
BiSwitch02	Fa0/3	SSCC088	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.13
BiSwitch02	Fa0/4	SSCC089	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.14
BiSwitch02	Fa0/5	SSCC090	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.15
BiSwitch02	Fa0/6	SSCC091	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.16
BiSwitch02	Fa0/7	SSCC092	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.17
BiSwitch02	Fa0/8	SSCC093	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.18
BiSwitch02	Fa0/9	SSCC094	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.19
BiSwitch02	Fa0/10	SSCC095	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.20
BiSwitch02	Fa0/11	SSCC096	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.21
BiSwitch02	Fa0/12	SSCC097	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 1.22
BiSwitch02	Fa0/13	SSCC098	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.01
BiSwitch02	Fa0/14	SSCC099	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.02
BiSwitch02	Fa0/15	SSCC100	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.03
BiSwitch02	Fa0/16	SSCC101	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.04
BiSwitch02	Fa0/17	IMPRESORA68205	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.05
BiSwitch02	Fa0/18	IMPRESORA68206	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.06
BiSwitch02	Fa0/19	IMPRESORA68207	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.07
BiSwitch02	Fa0/20	SSCC101	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.08
BiSwitch02	Fa0/21	SSCC102	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.09
BiSwitch02	Fa0/22	SSCC103	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.10
BiSwitch02	Fa0/23	SSCC104	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.11
BiSwitch02	Fa0/24	SSCC105	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.12
BiSwitch02	Gi0/1	Conectado BiSwitch03	1000	FULL	FWD	NO	Si	NO	Trunk	-----
BiSwitch02	Gi0/2	Conectado BiSwitch01	1000	FULL	FWD	NO	Si	NO	Trunk	-----

Tabla C-24 BiSwitch02

Catalyst 2960 10.239.68.243	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN	Información de la localización
BiSwitch03	Fa0/1	SSCC106	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.13
BiSwitch03	Fa0/2	SSCC107	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.14
BiSwitch03	Fa0/3	SSCC108	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.15
BiSwitch03	Fa0/4	SSCC109	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.16
BiSwitch03	Fa0/5	SSCC110	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.17
BiSwitch03	Fa0/6	SSCC111	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.18
BiSwitch03	Fa0/7	SSCC112	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.19
BiSwitch03	Fa0/8	SSCC113	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.20
BiSwitch03	Fa0/9	SSCC114	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.21
BiSwitch03	Fa0/10	SSCC115	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.22
BiSwitch03	Fa0/11	SSCC116	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.23
BiSwitch03	Fa0/12	SSCC117	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 2.24
BiSwitch03	Fa0/13	SSCC117	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 3.03
BiSwitch03	Fa0/14	SSCC118	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 3.04
BiSwitch03	Fa0/15	IMPRESORA68208	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 3.05
BiSwitch03	Fa0/16	SSCC119	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 3.06
BiSwitch03	Fa0/17	SSCC120	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 3.08
BiSwitch03	Fa0/18	SSCC121	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 3.07
BiSwitch03	Fa0/19	SSCC122	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 3.08
BiSwitch03	Fa0/20	SSCC123	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 3.09
BiSwitch03	Fa0/21	IMPRESORA68209	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 3.10
BiSwitch03	Fa0/22	BiSAI1	100	FULL	FWD	Si	NO	NO	5	Patch Panel de Bilbao 3.11
BiSwitch03	Fa0/23	APAGADA	-----	-----	-----	-----	-----	-----	5	Patch Panel de Bilbao 3.12
BiSwitch03	Fa0/24	APAGADA	-----	-----	-----	-----	-----	-----	5	Patch Panel de Bilbao 3.13
BiSwitch03	Gi0/1	Conectado BiSwitch01	1000	FULL	FWD	NO	Si	NO	Trunk	-----
BiSwitch03	Gi0/2	Conectado BiSwitch02	1000	FULL	BLK	NO	Si	NO	Trunk	-----

Tabla C-25 BiSwitch03

Catalyst 2960 10.239.69.241	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN	Información de la localización
OdSwitch41	Fa0/1	SSCC140	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D1
OdSwitch41	Fa0/2	SSCC141	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D2
OdSwitch41	Fa0/3	SSCC142	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D3
OdSwitch41	Fa0/4	SSCC143	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D4
OdSwitch41	Fa0/5	SSCC144	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D5
OdSwitch41	Fa0/6	SSCC145	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D6
OdSwitch41	Fa0/7	IMPRESORA69204	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D7
OdSwitch41	Fa0/8	APAGADO	-----	-----	-----	-----	-----	-----	6	Patch Panel de Bilbao D8
OdSwitch41	Fa0/9	APAGADO	-----	-----	-----	-----	-----	-----	6	Patch Panel de Bilbao D9
OdSwitch41	Fa0/10	IMPRESORA69200	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D10
OdSwitch41	Fa0/11	IMPRESORA69201	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D11
OdSwitch41	Fa0/12	SSCC146	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D12
OdSwitch41	Fa0/13	SSCC147	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D13
OdSwitch41	Fa0/14	SSCC148	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D14
OdSwitch41	Fa0/15	SSCC149	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D15
OdSwitch41	Fa0/16	SSCC150	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D16
OdSwitch41	Fa0/17	SSCC151	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D17
OdSwitch41	Fa0/18	SSCC152	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D18
OdSwitch41	Fa0/19	SSCC153	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D19
OdSwitch41	Fa0/20	SSCC154	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D20
OdSwitch41	Fa0/21	SSCC155	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D21
OdSwitch41	Fa0/22	SSCC156	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D22
OdSwitch41	Fa0/23	OdSAI1	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D23
OdSwitch41	Fa0/24	PuenteOdonell	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao Antena
	Gi0/1	Conectado OdSwitch02	1000	FULL	FWD	NO	Si	NO	Trunk	-----
	Gi0/2	Conectado OdSwitch02	1000	FULL	FWD	NO	Si	NO	Trunk	-----

Tabla C-26 OdSwitch01

Catalyst 2960 10.239.69.242	Puerto	Descripción	Velocidad	Duplex	Estado STP	PortFast	Trunk	EtherChannel	VLAN	Información de la localización
OdSwitch42	Fa0/1	SSCC157	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D25
OdSwitch42	Fa0/2	SSCC158	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D26
OdSwitch42	Fa0/3	IMPRESORA69202	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D27
OdSwitch42	Fa0/4	SSCC159	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D28
OdSwitch42	Fa0/5	SSCC160	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D29
OdSwitch42	Fa0/6	SSCC161	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D29
OdSwitch42	Fa0/7	SSCC162	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D30
OdSwitch42	Fa0/8	APAGADO	-----	-----	-----	-----	-----	-----	6	Patch Panel de Bilbao D31
OdSwitch42	Fa0/9	IMPRESORA69203	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D32
OdSwitch42	Fa0/10	SSCC163	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D33
OdSwitch42	Fa0/11	SSCC164	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D34
OdSwitch42	Fa0/12	SSCC165	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D35
OdSwitch42	Fa0/13	SSCC166	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D36
OdSwitch42	Fa0/14	SSCC167	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D37
OdSwitch42	Fa0/15	SSCC168	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D38
OdSwitch42	Fa0/16	SSCC169	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D39
OdSwitch42	Fa0/17	SSCC170	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D40
OdSwitch42	Fa0/18	SSCC171	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D41
OdSwitch42	Fa0/19	SSCC172	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D42
OdSwitch42	Fa0/20	SSCC173	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D43
OdSwitch42	Fa0/21	SSCC174	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D44
OdSwitch42	Fa0/22	SSCC175	100	FULL	FWD	Si	NO	NO	6	Patch Panel de Bilbao D45
OdSwitch42	Fa0/23	APAGADO	-----	-----	-----	-----	-----	-----	6	Patch Panel de Bilbao D46
OdSwitch42	Fa0/24	APAGADO	-----	-----	-----	-----	-----	-----	6	Patch Panel de Bilbao D47
OdSwitch42	Gi0/1	Conectado OdSwitch01	1000	FULL	FWD	NO	Si	NO	Trunk	-----
OdSwitch42	Gi0/2	Conectado OdSwitch01	1000	FULL	FWD	NO	Si	NO	Trunk	-----

Tabla C-27 OdSwitch02

Anexo D. Direccionamiento de las futuras DD.PP.

D.1 Calcular redes VLSM para las DD.PP.

Este anexo resume el procedimiento para calcular el direccionamiento previsto para las futuras DD.PP. que pertenecerán a la red del IATE. El proceso es similar al descrito en el capitulo 3 para el cálculo del direccionamiento aplicado a SS.CC.

Hay que recordar que en el capitulo 3 se obtuvieron las redes VLSM para el IATE, considerando 8 nuevas DD.PP. Los resultados de dividir en subredes la dirección asignada 10.239.64.0/18 fueron los siguientes:

DIRECCIÓN ASIGNADA	SUBREDES	DESCRIPCIÓN
10.239.64.0/18	10.239.64.0/21	**SS.CC.**
	10.239.72.0/21	**Futura Sede #2 del IATE**
	10.239.80.0/21	**Futura Sede #3 del IATE**
	10.239.88.0/21	**Futura Sede #4 del IATE**
	10.239.96.0/21	**Futura Sede #5 del IATE**
	10.239.104.0/21	**Futura Sede #6 del IATE**
	10.239.112.0/21	**Futura Sede #7 del IATE**
	10.239.120.0/21	**Futura Sede #8 del IATE**

Tabla D- 1 Redes VLSM para la futura red del IATE

Además, el cliente facilitó como datos de partida que el número de trabajadores en cada DD.PP. se estima alrededor de 40 y que en cada una de ellas se necesitarán cuatro divisiones: usuarios, Informática, Servidores y Wireless. Con esta información es evidente que sería suficiente con 2 bits del tercer octeto para identificar cada VLAN. Sin embargo, se ha decidido sobredimensionar con 3 bits, de tal modo que aunque en principio solo se requerirán 4 VLANs, se puedan reservar otras 4 para posibles usos futuros aún no especificados.

También en el capitulo 3 se cálculo el número de direcciones IP necesarias considerando una reserva adicional del 30% para cada sede.

SEDE	EQUIPOS	RESERVA	TOTAL DE EQUIPOS
SS.CC.	147	30%	192
Cádiz	40	30%	52
Huelva	40	30%	52
Granada	40	30%	52
Jaén	40	30%	52
Almería	40	30%	52
Córdoba	40	30%	52
Málaga	40	30%	52

Tabla D- 2 Requisitos de direcciones IP por DD.PP.

No hay que olvidar que SS.CC. completó todas las direcciones de la red 10.239.64.0/21, así que la siguiente dirección disponible es 10.239.72.0/21, asignada a la DD.PP de Cádiz. Según la tabla anterior, la sede de Cádiz requerirá 52 hosts. Habría que usar 6 bits, dado que $2^6 - 2 = 62$ direcciones de hosts utilizables. Al igual que en SS.CC., al tratarse de direccionamiento privado, no será un problema reservar un numero elevado de IP por VLAN, por tanto se utilizarán los 8 bits del cuarto octeto para las direcciones de hosts, quedando la representación binaria de bits disponibles y el resultado de la división en subredes para la sede de Cádiz como sigue:

		TERCER OCTETO								CUARTO OCTETO							
10.	239.	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0
RED	SUBRED			Sede #2			VLAN ##			HOST ##							
				SUBRED VLSM													

Tabla D- 3 Representación binaria de bits disponibles para la DD.PP de Cádiz.

DIRECCIÓN ASIGNADA A SEDE #2	SUBREDES DENTRO DE SEDE #2	RED / SUBRED		Sede #2 Cádiz	Vlan ##	HOST	DESCRIPCIÓN VLAN ## DD.PP. CÁDIZ
10.239.72.0/21	10.239.72.0/24	10. 239.	01	001	000	00000000	**VLAN #1** Usuarios
	10.239.73.0/24				001		**VLAN #2**

							Informática
	10.239.74.0/24				010		**VLAN #3** Servidores
	10.239.75.0/24				011		**VLAN #4** Wireless
	10.239.76.0/24				100		**VLAN #5** *(Uso futuro)*
	10.239.77.0/24				101		**VLAN #6** *(Uso futuro)*
	10.239.78.0/24				110		**VLAN #7** *(Uso futuro)*
	10.239.79.0/24				111		**VLAN #8** *(Uso futuro)*

Tabla D- 4 Cálculo de redes VLSM para DD.PP. de Cádiz.

El procedimiento es análogo para el resto de DD.PP y su resultado está recogido a modo de resumen en las tablas mostradas a continuación.

SEDE #3 – DD.PP. HUELVA																	
10.	239.	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
RED / SUBRED				Sede #3			Vlan ##			HOST ##							

Dirección Asignada a Sede #3	**Subredes dentro de Sede #3**	**Descripción VLANs de Sede #3**	
10.239.80.0/21	10.239.80.0/24	Usuarios	**VLAN #1**
	10.239..81.0/24	Informática	**VLAN #2**
	10.239.82.0/24	Servidores	**VLAN #3**
	10.239.83.0/26	Wireless	**VLAN #4**
	10.239.84.0/24	*(Uso futuro)*	**VLAN #5**
	10.239..85.0/24	*(Uso futuro)*	**VLAN #6**
	10.239.86.0/24	*(Uso futuro)*	**VLAN #7**
	10.239.87.0/26	*(Uso futuro)*	**VLAN #8**

Tabla D- 5 Cálculo de redes VLSM para DD.PP. de Huelva.

SEDE #4 – DD.PP. GRANADA																	
10.	239.	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0
RED / SUBRED				Sede #4			Vlan ##			HOST ##							

Dirección Asignada a Sede #4	Subredes dentro de Sede #4	Descripción VLANs de Sede #4	
10.239.88.0/21	10.239.88.0/24	Usuarios	**VLAN #1**
	10.239.89.0/24	Informática	**VLAN #2**
	10.239.90.0/26	Servidores	**VLAN #3**
	10.239.91.0/26	Wireless	**VLAN #4**
	10.239.92.0/24	*(Uso futuro)*	**VLAN #5**
	10.239.93.0/24	*(Uso futuro)*	**VLAN #6**
	10.239.94.0/26	*(Uso futuro)*	**VLAN #7**
	10.239.95.0/26	*(Uso futuro)*	**VLAN #8**

Tabla D- 6 Cálculo de redes VLSM para DD.PP. de Granada.

SEDE #5 – DD.PP. JAÉN																	
10.	239.	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
RED / SUBRED				Sede #5			Vlan ##			HOST ##							

Dirección Asignada a Sede #5	Subredes dentro de Sede #5	Descripción VLANs de Sede #5	
10.239.96.0/21	10.239.96.0/24	Usuarios	**VLAN #1**
	10.239.97.0/24	Informática	**VLAN #2**
	10.239.98.0/24	Servidores	**VLAN #3**
	10.239.99.0/24	Wireless	**VLAN #4**
	10.239.100.0/24	*(Uso futuro)*	**VLAN #5**
	10.239.101.0/24	*(Uso futuro)*	**VLAN #6**
	10.239.102.0/26	*(Uso futuro)*	**VLAN #7**
	10.239.103.0/26	*(Uso futuro)*	**VLAN #8**

Tabla D- 7 Cálculo de redes VLSM para DD.PP. de Jáen.

SEDE #6 – DD.PP. ALMERÍA																	
10.	239.	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
RED / SUBRED				Sede #6			Vlan ##			HOST ##							

Dirección Asignada a Sede #6	Subredes dentro de Sede #6	Descripción VLANs de Sede #6	
10.239.104.0/21	10.239.104.0/24	Usuarios	**VLAN #1**
	10.239.105.0/24	Informática	**VLAN #2**
	10.239.106.0/24	Servidores	**VLAN #3**
	10.239.107.0/26	Wireless	**VLAN #4**
	10.239.108.0/24	*(Uso futuro)*	**VLAN #5**
	10.239.109.0/24	*(Uso futuro)*	**VLAN #6**
	10.239.110.0/24	*(Uso futuro)*	**VLAN #7**
	10.239.111.0/26	*(Uso futuro)*	**VLAN #8**

Tabla D- 8 Cálculo de redes VLSM para DD.PP. de Almería.

SEDE #7 – DD.PP. CÓRDOBA																	
10.	239.	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
RED / SUBRED				Sede #7			Vlan ##			HOST ##							

Dirección Asignada a Sede #7	Subredes dentro de Sede #7	Descripción VLANs de Sede #7	
10.239.112.0/21	10.239.112.0/24	Usuarios	**VLAN #1**
	10.239.113.0/24	Informática	**VLAN #2**
	10.239.114.0/24	Servidores	**VLAN #3**
	10.239.115.0/24	Wireless	**VLAN #4**
	10.239.116.0/24	*(Uso futuro)*	**VLAN #5**
	10.239.117.0/24	*(Uso futuro)*	**VLAN #6**
	10.239.118.0/24	*(Uso futuro)*	**VLAN #7**
	10.239.119.0/24	*(Uso futuro)*	**VLAN #8**

Tabla D- 9 Cálculo de redes VLSM para DD.PP. de Córdoba.

SEDE #8 – DD.PP. MÁLAGA																
10.	239.	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0
RED / SUBRED				Sede #8			Vlan ##			HOST ##						

Dirección Asignada a Sede #8	Subredes dentro de Sede #8	Descripción VLANs de Sede #8	
10.239.120.0/21	10.239.120.0/24	Usuarios	**VLAN #1**
	10.239.121.0/24	Informática	**VLAN #2**
	10.239.122.0/24	Servidores	**VLAN #3**
	10.239.123.0/24	Wireless	**VLAN #4**
	10.239.124.0/24	*(Uso futuro)*	**VLAN #5**
	10.239.125.0/24	*(Uso futuro)*	**VLAN #6**
	10.239.126.0/24	*(Uso futuro)*	**VLAN #7**
	10.239.127.0/24	*(Uso futuro)*	**VLAN #8**

Tabla D- 10 Cálculo de redes VLSM para DD.PP. de Málaga.

La siguiente figura resume gráficamente los resultados obtenidos en los puntos desarrollados anteriormente.

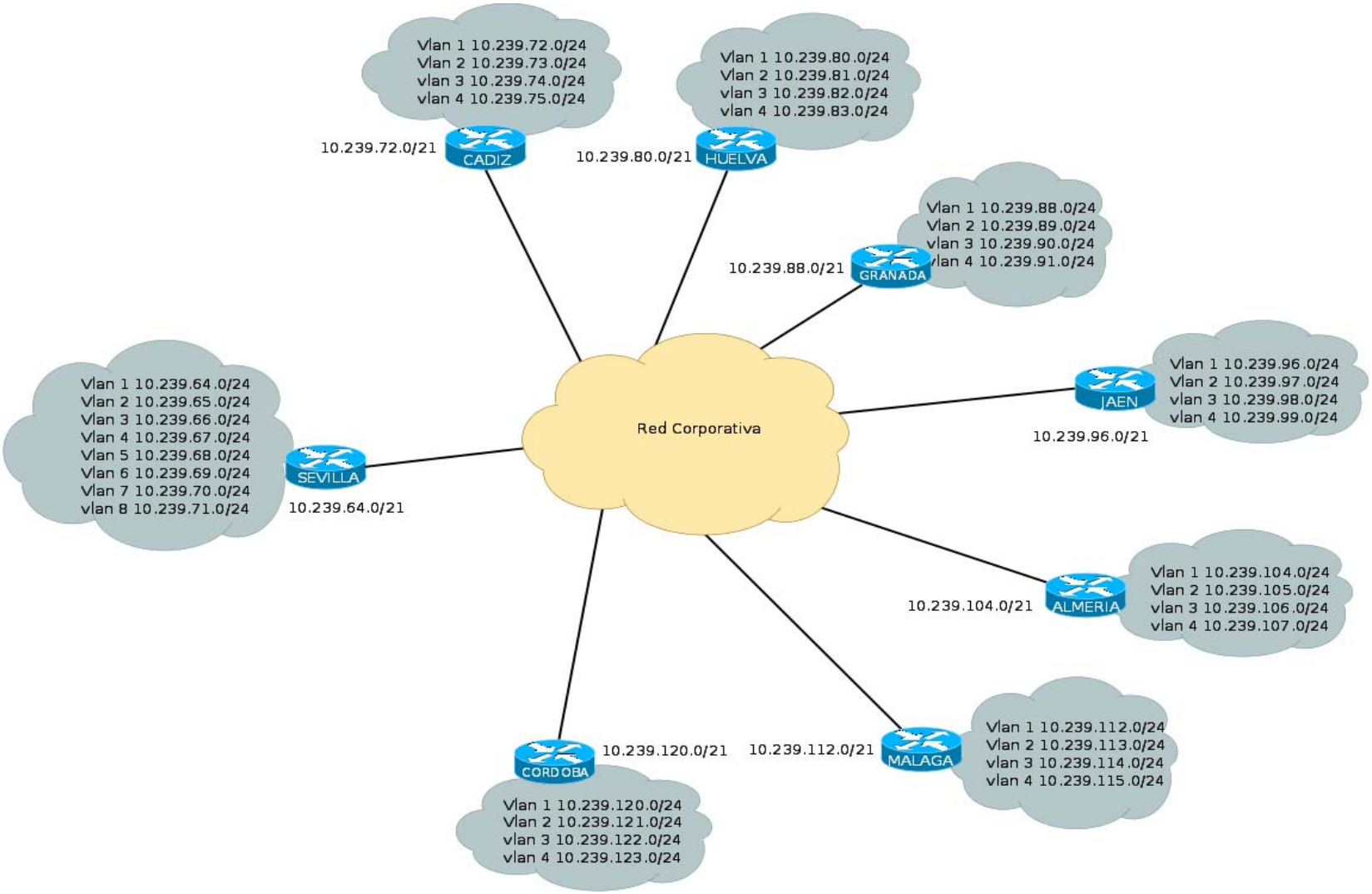


Figura D- 1Diseño en VLANs para la futura red del IATE

Bibliografía y referencias

- Academia de Networking de Cisco Systems. "*Guía del primer año. CCNA 1 y 2*". Tercera Edición, Madrid 2004. Editorial Pearson educación, S.A.

- Academia de Networking de Cisco Systems. "*Guía del primer año. CCNA 3 y 4*". Tercera Edición, Madrid 2004. Editorial Pearson educación, S.A.

- Academia de Networking de Cisco Systems. "*Fundamentos de Seguridad de Redes*". Madrid 2005. Editorial Pearson educación, S.A.

- Academia de Networking de Cisco Systems. "*Fundamentos de redes inalámbricas*". Madrid 2006. Editorial Pearson educación, S.A.

- Diane Teare. "*Designing for Cisco Internetwork Solutions (DESGN)*", 2008. Cisco Press.

- Keith Strassberg, Richard Gondek y Gary Rollie. "*Firewall. Manual de referencia*", Madrid 2003. Editorial Mc-GrawHill

- Craig Zacker. "*Redes. Manual de referencia*". Editorial Mc-GrawHill

- Richard Bejtlich. "*El Tao de la monitorización de seguridad en redes*". Madrid, 2005. Editorial Pearson educación, S.A

- William Stalling. "*Comunicaciones y redes de computadoras*", Junio 2007. Editorial Prentice Hall.

- Eric Vyncke y Christopher Paggen. "*LAN switch security what hackers Know About your Switches*", 2008. Cisco Press.

- Priscilla Oppenheimer. "*Top-Down Network Design Second Edition*", Mayo 2004. Cisco Press

- William Pollock. "*Nagios System and Network Monitoring*", Munich 2005. Publicado por Open Source Press GmbH.

- Antonio Villalón. “S*eguridad en unix y redes”*

Otras referencias utilizadas:

- http://cisco.netacad.net

  Página oficial de la academia de Cisco System

- http://www.nagios.org/

  Pagina oficial de Nagios

- http://www.cacti.net/

  Pagina oficial de Cacti

- http://www.ntop.org/

  Pagina oficial de Ntop